Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/015085

International filing date: 18 August 2005 (18.08.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-239465
Filing date: 19 August 2004 (19.08.2004)

Date of receipt at the International Bureau: 13 October 2005 (13.10.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出　願　年　月　日
Date of Application:　２００４年　８月１９日

出　願　番　号
Application Number:　特願２００４－２３９４６５

パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is　ＪＰ２００４－２３９４６５

出　願　人
Applicant(s):　日本電信電話株式会社

２００５年　９月２８日

特許庁長官
Commissioner,
Japan Patent Office　中嶋　誠

【書類名】　特許願
【整理番号】　NTTH165228
【提出日】　平成16年 8月19日
【あて先】　特許庁長官殿
【国際特許分類】　G09C 1/00
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　堀田　英一
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　小野　諭
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　石本　英隆
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　田倉　昭
【特許出願人】
　【識別番号】　000004226
　【氏名又は名称】　日本電信電話株式会社
【代理人】
　【識別番号】　100083806
　【弁理士】
　【氏名又は名称】　三好　秀和
　【電話番号】　03-3504-3075
【手数料の表示】
　【予納台帳番号】　001982
　【納付金額】　16,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9701396

【書類名】特許請求の範囲
【請求項１】
所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの前記要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記証明装置のイベント順序証明方法であって、
前記利用者装置からの前記要求を受信する順序証明要求受信ステップと、
前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算ステップと、
前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約ステップと、
前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第１の順次集約木特定情報を含む証明書を作成する証明書作成ステップと、
前記証明書を前記利用者装置に送信する証明書送信ステップと、
前記利用者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、
前記利用者装置からの前記要求を前記順次集約木に割り当てた以後に、監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、監査用証明書を作成するとともに、前記監査用の前記要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、該監査用証明書に含める監査用証明書作成ステップと、
前記監査用証明書を前記監査装置に送信する監査用証明書送信ステップと、
前記監査用の要求を前記順次集約木に割り当てた以後に、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信ステップと、
前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第２の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成ステップと、
前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信ステップと、
を有することを特徴とするイベント順序証明方法。
【請求項２】
前記証明書は、前記証明書の即時補完情報を含むことを特徴とする請求項１記載のイベント順序証明方法。
【請求項３】
前記監査用証明書作成ステップは、さらに、前記利用者装置からの前記要求を前記順次集約木に割り当てた以前に、監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、監査用証明書を作成するとともに、前記監査用の前記要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、該監査用証明書に含めるステップを備え、
前記一定時間間隔終了後に前記監査用証明書作成ステップで作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成ステップと、
前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信

ステップと、
を有することを特徴とする請求項１又は２記載のイベント順序証明方法。
【請求項４】
前記順次割当データは、前記要求に含まれるデジタル情報に対して所定の衝突困難一方向関数を適用した結果値であることを特徴とする請求項１乃至３のいずれか1項に記載のイベント順序証明方法。
【請求項５】
前記証明書は、デジタル署名が施されていることを特徴とする請求項1乃至４のいずれか1項に記載のイベント順序証明方法。
【請求項６】
前記一定時間間隔終了後に前記順次集約木のルート値を電子的に公表する電子的情報公表ステップを有することを特徴とする請求項1乃至５のいずれか1項に記載のイベント順序証明方法。
【請求項７】
前記証明装置は、複数の前記要求を前記順次集約木に順次割り当てたときは、割り当てた時間的順序で、前記複数の要求に対する証明書を送信する手段を有することを特徴とする請求項1乃至６のいずれか1項に記載のイベント順序証明方法。
【請求項８】
所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの該要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記監査装置のイベント順序証明監査方法であって、
前記証明装置は、
前記利用者装置からの前記要求を受信する順序証明要求受信手段と、
前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、
前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、
前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第１の順次集約木特定情報を含む証明書を作成する証明書作成手段と、
前記証明書を前記利用者装置に送信する証明書送信手段と、
前記利用者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、
複数の監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、前記複数の監査用の前記要求を前記順次集約木に割り当てた時点におけるそれぞれの監査用の前記即時補完情報を前記順次集約木から取得し、前記複数の監査用証明書に含める監査用証明書作成手段と、
前記監査用証明書を前記監査装置に送信する監査用証明書送信手段と、
前記証明書送信後、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、
前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第２の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取

得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、
　前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、
を有し、
　前記証明装置から、前記複数の監査用証明書を受信する監査用証明書受信ステップと、
　前記利用者装置から、前記証明書及び前記遅延補完情報を含む前記証明書に対する監査要求を受信する監査要求受信ステップと、
　受信した複数の監査用証明書の中から、受信した監査要求の第１及び第２の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より生成された時間的順序が後、かつ遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第１の監査用証明書選択ステップと、
　前記順次集約木の特定のノードに対して、前記第１の監査用証明書選択ステップで選択された監査用証明書に含まれる該ノードの割当値と、前記監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第１の証明書監査ステップと、
　前記証明書の監査結果を前記利用者装置に送信する監査結果送信ステップと、
を有することを特徴とするイベント順序証明監査方法。
【請求項９】
　前記監査用証明書受信ステップは、前記監査用証明書を受信する第１の時刻を時刻提供装置から取得するステップを有し、
　前記第１の証明書監査ステップは、前記証明書の要求受付が前記第１の時刻よりも時間的に前であることを示す区間時刻証を監査結果に含めることを特徴とする請求項８記載のイベント順序証明監査方法。
【請求項１０】
　前記証明装置は、
前記一定時間間隔終了後に前記監査用証明書作成手段で作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、
　前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、
を有し、
　受信した複数の監査用証明書の中から、受信した監査要求の第１の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より時間的順序が前の監査用証明書を選択する第２の監査用証明書選択ステップと、
　前記順次集約木の特定のノードに対して、前記監査要求に含まれる該ノードの割当値と、前記第２の監査用証明書選択ステップで選択された監査用証明書及び該監査用証明書の遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第２の証明書監査ステップと、
を有することを特徴とする請求項８又は９記載のイベント順序証明監査方法。
【請求項１１】
　複数の証明書に対する各監査結果と、前記複数の証明書の第１の順次集約木特定情報に基づいて、前記複数の証明書間における要求受付の時間的順序を判定する利用者間順序判定ステップと、を有し、
　前記監査結果送信ステップは、前記複数の証明書間における要求受付の時間的順序を前記監査結果に含めることを特徴とする請求項１０記載のイベント順序証明監査方法。
【請求項１２】
　前記監査用証明書及び該監査用証明書の遅延補完情報から前記順次集約木のルート値を計算するルート値計算ステップと、

電子的に公表された前記順次集約木のルート値と計算されたルート値が一致するか否かの検証を行うルート値検証ステップと、
を有することを特徴とする請求項１０又は１１記載のイベント順序証明監査方法。
【請求項１３】
前記第１の監査用証明書選択ステップで選択された監査用証明書及び該監査用証明書の遅延補完情報を前記利用者装置に送信する監査用補完情報送信ステップを有することを特徴とする請求項１０乃至１２のいずれか１項に記載のイベント順序証明監査方法。
【請求項１４】
前記監査用証明書受信ステップは、監査用の前記要求を前記証明装置に送信する第２の時刻を時刻提供装置から取得するステップを有し、
前記第２の証明書監査ステップは、前記証明書の要求受付が前記第２の時刻より時間的に後であることを示す区間時刻証を監査結果に含めることを特徴とする請求項１０乃至１３のいずれか1項に記載のイベント順序証明監査方法。
【請求項１５】
前記監査結果は、デジタル署名が施されていることを特徴とする請求項８乃至１４のいずれか1項に記載のイベント順序証明監査方法。
【請求項１６】
所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの前記要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記証明装置であって、
前記利用者装置からの前記要求を受信する順序証明要求受信手段と、
前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、
前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、
前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第１の順次集約木特定情報を含む証明書を作成する証明書作成手段と、
前記証明書を前記利用者装置に送信する証明書送信手段と、
前記利用者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、
前記利用者装置からの前記要求を前記順次集約木に割り当てた以後に、監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、監査用証明書を作成するとともに、前記監査用の前記要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、該監査用証明書に含める監査用証明書作成手段と、
前記監査用証明書を前記監査装置に送信する監査用証明書送信手段と、
前記監査用の要求を前記順次集約木に割り当てた以後に、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、
前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第２の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、

前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、
を有することを特徴とする証明装置。
【請求項１７】
前記証明書は、前記証明書の即時補完情報を含むことを特徴とする請求項１６記載の証明装置。
【請求項１８】
前記監査用証明書作成手段は、さらに、前記利用者装置からの前記要求を前記順次集約木に割り当てた以前に、監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、監査用証明書を作成するとともに、前記監査用の前記要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、該監査用証明書に含める手段を備え、
前記一定時間間隔終了後に前記監査用証明書作成手段で作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、
前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、
を有することを特徴とする請求項１６又は１７記載の証明装置。
【請求項１９】
前記順次割当データは、前記要求に含まれるデジタル情報に対して所定の衝突困難一方向関数を適用した結果値であることを特徴とする請求項１６乃至１８のいずれか1項に記載の証明装置。
【請求項２０】
前記証明書は、デジタル署名が施されていることを特徴とする請求項１６乃至１９のいずれか1項に記載の証明装置。
【請求項２１】
前記一定時間間隔終了後に前記順次集約木のルート値を電子的に公表する電子的情報公表手段を有することを特徴とする請求項１６乃至２０のいずれか1項に記載の証明装置。
【請求項２２】
前記証明装置は、複数の前記要求を前記順次集約木に順次割り当てたときは、割り当てた時間的順序で、前記複数の要求に対する証明書を送信する手段を有することを特徴とする請求項16乃至２１のいずれか1項に記載の証明装置。
【請求項２３】
所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの該要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記監査装置であって、
前記証明装置は、
前記利用者装置からの前記要求を受信する順序証明要求受信手段と、
前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、
前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、
前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第１の順次集約木特定情報を含む証明書を作成する証明書作成手段と、
前記証明書を前記利用者装置に送信する証明書送信手段と、

前記利用者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、

複数の監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、前記複数の監査用の前記要求を前記順次集約木に割り当てた時点におけるそれぞれの監査用の前記即時補完情報を前記順次集約木から取得し、前記複数の監査用証明書に含める監査用証明書作成手段と、

前記監査用証明書を前記監査装置に送信する監査用証明書送信手段と、

前記証明書送信後、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、

前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第２の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、

前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、

を有し、

前記証明装置から、前記複数の監査用証明書を受信する監査用証明書受信手段と、

前記利用者装置から、前記証明書及び前記遅延補完情報を含む前記証明書に対する監査要求を受信する監査要求受信手段と、

受信した複数の監査用証明書の中から、受信した監査要求の第１及び第２の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より生成された時間的順序が後、かつ遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第１の監査用証明書選択手段と、

前記順次集約木の特定のノードに対して、前記第１の監査用証明書選択手段で選択された監査用証明書に含まれる該ノードの割当値と、前記監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第１の証明書監査手段と、

前記証明書の監査結果を前記利用者装置に送信する監査結果送信手段と、

を有することを特徴とする監査装置。

【請求項２４】

前記監査用証明書受信手段は、前記監査用証明書を受信する第１の時刻を時刻提供装置から取得する手段を有し、

前記第１の証明書監査手段は、前記証明書の要求受付が前記第１の時刻よりも時間的に前であることを示す区間時刻証を監査結果に含めることを特徴とする請求項２３記載の監査装置。

【請求項２５】

前記証明装置は、

前記一定時間間隔終了後に前記監査用証明書作成手段で作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、

前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、

を有し、

受信した複数の監査用証明書の中から、受信した監査要求の第１の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より時間的順序が前の監査用証明書を選択する第２の監査用証明書選択手段と、

前記順次集約木の特定のノードに対して、前記監査要求に含まれる該ノードの割当値と、前記第２の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延

補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第２の証明書監査手段と、
を有することを特徴とする請求項２３又は２４記載の監査装置。
【請求項２６】
複数の証明書に対する各監査結果と、前記複数の証明書の第１の順次集約木特定情報に基づいて、前記複数の証明書間における要求受付の時間的順序を判定する利用者間順序判定手段と、を有し、
前記監査結果送信手段は、前記複数の証明書間における要求受付の時間的順序を前記監査結果に含めることを特徴とする請求項２５記載の監査装置。
【請求項２７】
前記監査用証明書及び該監査用証明書の遅延補完情報から前記順次集約木のルート値を計算するルート値計算手段と、
電子的に公表された前記順次集約木のルート値と計算されたルート値が一致するか否かの検証を行うルート値検証手段と、
を有することを特徴とする請求項２５又は２６記載の監査装置。
【請求項２８】
前記第１の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報を前記利用者装置に送信する監査用補完情報送信手段を有することを特徴とする請求項２５乃至２７のいずれか１項に記載の監査装置。
【請求項２９】
前記監査用証明書受信手段は、監査用の前記要求を前記証明装置に送信する第２の時刻を時刻提供装置から取得する手段を有し、
前記第２の証明書監査手段は、前記証明書の要求受付が前記第２の時刻より時間的に後であることを示す区間時刻証を監査結果に含めることを特徴とする請求項２５乃至２８のいずれか1項に記載の監査装置。
【請求項３０】
前記監査結果は、デジタル署名が施されていることを特徴とする請求項２５乃至２９のいずれか1項に記載の監査装置。
【請求項３１】
請求項１乃至７のいずれか１項に記載のイベント順序証明方法の各ステップを前記証明装置に実行させることを特徴とするイベント順序証明プログラム。
【請求項３２】
請求項８乃至１５のいずれか１項に記載のイベント順序証明監査方法の各ステップを前記証明監査装置に実行させることを特徴とするイベント順序証明監査プログラム。
【請求項３３】
所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの前記要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記利用者装置のためのイベント順序証明検証プログラムであって、
前記証明装置は、
前記利用者装置からの前記要求を受信する順序証明要求受信手段と、
前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、
前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する

順序証明要求集約手段と、
前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第１の順次集約木特定情報を含む証明書を作成する証明書作成手段と、
前記証明書を前記利用者装置に送信する証明書送信手段と、
前記利用者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、
複数の監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、前記複数の監査用の前記要求を前記順次集約木に割り当てた時点におけるそれぞれの監査用の前記即時補完情報を前記順次集約木から取得し、前記複数の監査用証明書に含める監査用証明書作成手段と、
前記監査用証明書を前記監査装置に送信する監査用証明書送信手段と、
前記証明書送信後、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、
前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第２の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、
前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、
を有し、
前記監査装置は、
前記証明装置から、前記複数の監査用証明書を受信する監査用証明書受信手段と、
前記利用者装置から、前記証明書及び前記遅延補完情報を含む前記証明書に対する監査要求を受信する監査要求受信手段と、
受信した複数の監査用証明書の中から、受信した監査要求の第１及び第２の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より生成された時間的順序が後、かつ遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第１の監査用証明書選択手段と、
前記順次集約木の特定のノードに対して、前記第１の監査用証明書選択手段で選択された監査用証明書に含まれる該ノードの割当値と、前記監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第１の証明書監査手段と、
前記証明書の監査結果を前記利用者装置に送信する監査結果送信手段と、
を有し、
前記要求を前記証明装置に送信する順序証明要求送信ステップと、
前記証明装置から、前記証明書を受信する証明書受信ステップと、
前記証明書の補完情報の要求を前記証明装置に送信する補完情報要求送信ステップと、
前記証明装置から、前記補完情報を受信する補完情報受信ステップと、
前記監査要求を前記監査装置に送信する監査要求送信ステップと、
前記監査結果を受信する監査結果受信ステップと、
を前記利用者装置に実行させることを特徴とするイベント順序証明検証プログラム。
【請求項３４】
前記監査装置の前記監査用証明書受信手段は、前記監査用証明書を受信する第１の時刻を時刻提供装置から取得する手段を有し、
前記第１の証明書監査手段は、前記証明書の要求受付が前記第１の時刻よりも時間的に前であることを示す区間時刻証を監査結果に含め、
前記要求を前記証明装置に送信する時点の第３の時刻を前記時刻提供装置から取得し、

該第３の時刻を所定の手順に従って計算した値を前記要求に含める順序証明要求作成ステップを
前記利用者装置に実行させることを特徴とする請求項３３記載のイベント順序証明検証プログラム。
【請求項３５】
前記証明装置は、
前記一定時間間隔終了後に前記監査用証明書作成手段で作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、
前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、
を有し、
前記監査装置は、
受信した複数の監査用証明書の中から、受信した監査要求の第１の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より時間的順序が前の監査用証明書を選択する第２の監査用証明書選択手段と、
前記順次集約木の特定のノードに対して、前記監査要求に含まれる該ノードの割当値と、前記第２の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第２の証明書監査手段と、
を有することを特徴とする請求項３３又は３４記載のイベント順序証明検証プログラム。
【請求項３６】
前記監査装置は、
複数の証明書に対する各監査結果と、前記複数の証明書の第１の順次集約木特定情報に基づいて、前記複数の証明書間における要求受付の時間的順序を判定する利用者間順序判定手段を有し、
前記監査結果送信手段は、前記複数の証明書間における要求受付の時間的順序を前記監査結果に含め、
前記監査要求は、他の証明書との時間的順序の判定要求を含むことを特徴とする請求項３５記載のイベント順序証明検証プログラム。
【請求項３７】
前記監査装置は、
前記第１の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報を前記利用者装置に送信する監査用補完情報送信手段を有し、
前記監査装置から送信された監査用証明書及び該監査用証明書の遅延補完情報を受信するステップを前記利用者装置に実行させることを特徴とする請求項３５記載のイベント順序証明検証プログラム。
【請求項３８】
前記監査用証明書受信手段は、監査用の前記要求を前記証明装置に送信する第２の時刻を時刻提供装置から取得する手段を有し、
第２の証明書監査手段は、前記証明書の要求受付が前記第２の時刻より時間的に後であることを示す区間時刻証を監査結果に含め、
前記要求を前記証明装置に送信する時点の第３の時刻を前記時刻提供装置から取得し、該第３の時刻を所定の手順に従って計算した値を前記要求に含める順序証明要求作成ステップを
前記利用者装置に実行させることを特徴とする請求項３４乃至３７のいずれか１項に記載のイベント順序証明検証プログラム。
【請求項３９】
前記証明装置から受信した証明書、及び前記一定時間間隔終了後に取得した該証明書の

補完情報すべてから、前記順次集約木のルート値を計算するルート値計算ステップと、
前記一定時間間隔終了後に電子的に公表された前記順次集約木のルート値と計算されたルート値が一致するか否かの検証を行うルート値検証ステップと、
を前記利用者装置に実行させることを特徴とする請求項３３乃至３８のいずれか１項に記載のイベント順序証明検証プログラム。
【請求項４０】
請求項３４又は３８記載のイベント順序証明検証プログラムを実行する利用者装置が前記要求に付した時刻を検証するコンピュータが読み取り可能なイベント時刻検証プログラムであって、
前記監査結果を取得する監査結果取得ステップと、
前記監査結果に対応する前記要求を取得する順序証明要求取得ステップと、
前記第３の時刻と、前記第１又は第２の時刻のうち少なくとも１以上との時間差に基づいて、前記第３の時刻の正当性を判定する時刻検証ステップと、
前記判定結果を出力するステップと、
前記コンピュータに実行させることを特徴とするイベント時刻検証プログラム。

【書類名】明細書
【発明の名称】イベント順序証明方法及びイベント順序証明監査方法、イベント順序証明システムにおける証明装置及び監査装置、並びにイベント順序証明プログラム、イベント順序証明監査プログラム、イベント順序証明検証プログラム及びイベント時刻検証プログラム
【技術分野】
【０００１】
本発明は、デジタル・データの生成を伴うイベントの生起順序を証明するイベント順序証明技術に関する。
【背景技術】
【０００２】
イベント順序証明技術は、デジタル・データの生成を伴う複数のイベントの間の生起順序を証明するとともに、そのようなイベントに伴って生成されたデジタル・データが何であったかを証明する技術である。
【０００３】
近年、インターネット上での電子商取引の活発化や、デジタル文書管理の利用拡大に伴い、「誰が、いつ、どんなデータを生成し、交信したか」を第三者が証明する電子公証の仕組みが必要とされている。電子公証は、送受信者の特定、到達確認、送受信等の前後関係の証明、改ざんの検知、電子文書保管等の機能を具備するものであるが、イベント順序証明技術は、このうち、前後関係の証明及び改ざんの検知の機能を実現するものである。
【０００４】
図32は、このようなイベント順序証明技術を用いたイベント順序証明システムを説明する図である。同図に示すイベント順序証明システム900は、利用者（要求者、検証者）80がイベント順序証明の対象データをイベント順序証明装置90に送信すると、イベント順序証明装置90が利用者80から要求された対象データに対して受付の順番を示すデータを付したイベント順序受理証明書を生成し、該イベント順序受理証明書を利用者に返信するようになっている。そして、イベント順序証明装置90で発行されたイベント順序受理証明書は、ＰＫＩ（Public Key Infrastructure；公開鍵基盤）のもとでデジタル署名を主要な偽造防止／証明手段として採用する場合には、一般に、利用者80から送られた対象データに受付の順番を付した署名対象データに対するデジタル署名を含んだイベント順序受理証明書となっている。
【０００５】
このイベント順序受理証明書の真正性の主要な根拠としてデジタル署名を用いるイベント順序証明システムに関しては、イベント順序証明装置 90の不正、イベント順序受理証明書の有効期間、およびシステム運用の面などにおいて問題点が指摘されている。そのため、イベント順序受理証明書の真正性の主要な根拠としてデジタル署名を用いないイベント順序証明の方法も提案されている。例えば、線形リンキング（Linear Linking Protocol）による方法（例えば、非特許文献１参照。）は、イベント順序証明装置90が仮に信頼できないとしてもシステム全体として高い安全性を確保することが可能となっている方法である。図33は、ＰＫＩに依存しない線形リンキングによるイベント順序証明システムを説明する図である。同図に示すイベント順序証明システム910は、複数の利用者80のイベント順序証明対象データ（ハッシュ値）を相互に関連付けるリンク情報L_nを生成し、リンク情報L_nを含むイベント順序受理証明書を返信するようになっており、各イベント順序受理証明書が、それまでに生成されたすべてのイベント順序受理証明書に依存するようになっている。そして、このリンク情報の一部（L_M，L_N）が定期的にマスメディア等（例えば新聞）に公表されるので、これにより、イベント順序証明装置90の不正を防止し、結果としてシステム全体の信頼を高めることができるようになっている。
【０００６】
この線形リンキングの方式については、イベント順序証明装置90の不正を検出するために利用者80相互の協力が必要であるという問題点、及び、利用者80が取得したイベント順

序受理証明書を検証、即ち、該イベント順序受理証明書と公表された情報が所定の方式で関係づけられることを検証するには利用者80はイベント順序証明装置90から大量のデータを取得する必要があるという問題点が指摘されている。

【０００７】

これらの問題の一部を解決するための方法も提案されている。例えば、非特許文献２においては、一定期間にイベント順序証明装置で処理されたイベント順序証明要求をまとめ公表するデータを計算するために、非特許文献１で使われている線形のリストの代わりに、木構造を用いることにより、利用者80がイベント順序受理証明書の検証を行うために必要なデータの量を、該一定期間に受付けられるイベント順序証明要求の数に比例する量から、その対数（底2）に比例する量に著しく削減する方法を提案している。

【非特許文献１】S. Haber and W. Stornetta, How to Time-Stamp a Digital Document, Journal of Cryptology, Vol. 3, No. 2, pp. 99—111, 1991

【非特許文献２】A. Buldas、H. Lipmaa and B. Schoenmakers, Optimally efficient accountable time-stamping, in Proceedings of Public Key Cryptography 2000 (PKC2000), eds. Y. Zheng and H. Imai, pp.293—305, Springer-Verlag, January 2000

【発明の開示】

【発明が解決しようとする課題】

【０００８】

しかしながら、上述した従来技術の木構造を用いる方式については、次のような問題点がある。

【０００９】

ある一定期間に異なる２つの利用者が各々イベント順序証明要求をイベント順序証明装置に送付し、それら要求が受理されたときにおいて、第１の利用者のある順序証明要求の受付けが第２の利用者のある順序証明要求の受付けより前になされたことの証明が、当該の期間が終了してイベント順序証明要求をまとめた公表データが公開されるまではできないという問題がある。即ち、当該の２つの順序証明要求と公表データが所定の方式で関係付けられることの検証が、公表データが公開されるまでできないという問題がある。このため、イベント順序証明システムに対する利用者の利便性が劣るとともに、イベント順序証明装置に障害が発生した時には、イベント順序受理証明書の検証ができないという欠点がある。

【００１０】

本発明は、上記の問題を解決するためになされたものであり、木構造を用いてイベント順序を証明するイベント順序証明システムにおいて、イベント順序証明要求をまとめた公表データを用いなくても、イベント順序証明機関から発行されたイベント順序受理証明書の検証を行うことができるイベント順序証明方法及びイベント順序証明監査方法、イベント順序証明システムにおける証明装置及び監査装置、並びにイベント順序証明プログラム、イベント順序証明監査プログラム、イベント順序証明検証プログラム及びイベント時刻検証プログラムを提供することを目的とする。

【課題を解決するための手段】

【００１１】

上記目的を達成するため、請求項１記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの前記要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記証明装置のイベント順序証明方法であって、前記利用者装置からの前記要求を受信する順序証明要求受信ステップと、前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算ステップと、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの

割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約ステップと、前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第１の順次集約木特定情報を含む証明書を作成する証明書作成ステップと、前記証明書を前記利用者装置に送信する証明書送信ステップと、前記利用者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、前記利用者装置からの前記要求を前記順次集約木に割り当てた以後に、監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、監査用証明書を作成するとともに、前記監査用の前記要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、該監査用証明書に含める監査用証明書作成ステップと、前記監査用証明書を前記監査装置に送信する監査用証明書送信ステップと、前記監査用の要求を前記順次集約木に割り当てた以後に、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信ステップと、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第２の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成ステップと、前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信ステップと、を有することを特徴とする。

【００１２】

請求項２記載の本発明は、請求項１記載の発明において、前記証明書は、前記証明書の即時補完情報を含むことを特徴とする。

【００１３】

請求項３記載の本発明は、請求項１又は２記載の発明において、前記監査用証明書作成ステップは、さらに、前記利用者装置からの前記要求を前記順次集約木に割り当てた以前に、監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、監査用証明書を作成するとともに、前記監査用の前記要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、該監査用証明書に含めるステップを備え、前記一定時間間隔終了後に前記監査用証明書作成ステップで作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成ステップと、前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信ステップと、を有することを特徴とする。

【００１４】

請求項４記載の本発明は、請求項１乃至３のいずれか１項に記載の発明において、前記順次割当データは、前記要求に含まれるデジタル情報に対して所定の衝突困難一方向関数を適用した結果値であることを特徴とする。

【００１５】

請求項５記載の本発明は、請求項１乃至４のいずれか１項に記載の発明において、前記証明書は、デジタル署名が施されていることを特徴とする。

【００１６】

請求項６記載の本発明は、請求項１乃至５のいずれか１項に記載の発明において、前記一定時間間隔終了後に前記順次集約木のルート値を電子的に公表する電子的情報公表ステップを有することを特徴とする。

【００１７】

請求項７記載の本発明は、請求項１乃至６のいずれか１項に記載の発明において、前記証明装置は、複数の前記要求を前記順次集約木に順次割り当てたときは、割り当てた時間的順序で、前記複数の要求に対する証明書を送信する手段を有することを特徴とする。

【００１８】

請求項８記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの該要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記監査装置のイベント順序証明監査方法であって、前記証明装置は、前記利用者装置からの前記要求を受信する順序証明要求受信手段と、前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第１の順次集約木特定情報を含む証明書を作成する証明書作成手段と、前記証明書を前記利用者装置に送信する証明書送信手段と、前記利用者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、複数の監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、前記複数の監査用の前記要求を前記順次集約木に割り当てた時点におけるそれぞれの監査用の前記即時補完情報を前記順次集約木から取得し、前記複数の監査用証明書に含める監査用証明書作成手段と、前記監査用証明書を前記監査装置に送信する監査用証明書送信手段と、前記証明書送信後、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第２の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、を有し、前記証明装置から、前記複数の監査用証明書を受信する監査用証明書受信ステップと、前記利用者装置から、前記証明書及び前記遅延補完情報を含む前記証明書に対する監査要求を受信する監査要求受信ステップと、受信した複数の監査用証明書の中から、受信した監査要求の第１及び第２の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より生成された時間的順序が後、かつ遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第１の監査用証明書選択ステップと、前記順次集約木の特定のノードに対して、前記第１の監査用証明書選択ステップで選択された監査用証明書に含まれる該ノードの割当値と、前記監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第１の証明書監査ステップと、前記証明書の監査結果を前記利用者装置に送信する監査結果送信ステップと、を有することを特徴とする。

【００１９】

請求項９記載の本発明は、請求項８記載の発明において、前記監査用証明書受信ステップは、前記監査用証明書を受信する第１の時刻を時刻提供装置から取得するステップを有し、前記第１の証明書監査ステップは、前記証明書の要求受付が前記第１の時刻よりも時間的に前であることを示す区間時刻証を監査結果に含めることを特徴とする。

【００２０】

請求項１０記載の本発明は、請求項８又は９記載の発明において、前記証明装置は、前記一定時間間隔終了後に前記監査用証明書作成手段で作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延

補完情報作成手段と、前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、を有し、受信した複数の監査用証明書の中から、受信した監査要求の第１の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より時間的順序が前の監査用証明書を選択する第２の監査用証明書選択ステップと、前記順次集約木の特定のノードに対して、前記監査要求に含まれる該ノードの割当値と、前記第２の監査用証明書選択ステップで選択された監査用証明書及び該監査用証明書の遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第２の証明書監査ステップと、を有することを特徴とする。

【００２１】

請求項１１記載の本発明は、請求項１０記載の発明において、複数の証明書に対する各監査結果と、前記複数の証明書の第１の順次集約木特定情報に基づいて、前記複数の証明書間における要求受付の時間的順序を判定する利用者間順序判定ステップと、を有し、前記監査結果送信ステップは、前記複数の証明書間における要求受付の時間的順序を前記監査結果に含めることを特徴とする。

【００２２】

請求項１２記載の本発明は、請求項１０又は１１記載の発明において、前記監査用証明書及び該監査用証明書の遅延補完情報から前記順次集約木のルート値を計算するルート値計算ステップと、電子的に公表された前記順次集約木のルート値と計算されたルート値が一致するか否かの検証を行うルート値検証ステップと、を有することを特徴とする。

【００２３】

請求項１３記載の本発明は、請求項１０乃至１２のいずれか１項に記載の発明において、前記第１の監査用証明書選択ステップで選択された監査用証明書及び該監査用証明書の遅延補完情報を前記利用者装置に送信する監査用補完情報送信ステップを有することを特徴とする。

【００２４】

請求項１４記載の本発明は、請求項１０乃至１３のいずれか1項に記載の発明において、前記監査用証明書受信ステップは、監査用の前記要求を前記証明装置に送信する第２の時刻を時刻提供装置から取得するステップを有し、前記第２の証明書監査ステップは、前記証明書の要求受付が前記第２の時刻より時間的に後であることを示す区間時刻証を監査結果に含めることを特徴とする。

【００２５】

請求項１５記載の本発明は、請求項８乃至１４のいずれか1項に記載の発明において、前記監査結果は、デジタル署名が施されていることを特徴とする。

【００２６】

請求項１６記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの前記要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記証明装置であって、前記利用者装置からの前記要求を受信する順序証明要求受信手段と、前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第１の順次集約木特定情報を含む証明書を作成する証明書作成手段と、前記証明書を前記利用者装置に送信する証明書送信手段と、前記利用者装置からの前記要求が割り当てられた前記順次集約木のリー

フからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、前記利用者装置からの前記要求を前記順次集約木に割り当てた以後に、監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、監査用証明書を作成するとともに、前記監査用の前記要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、該監査用証明書に含める監査用証明書作成手段と、前記監査用証明書を前記監査装置に送信する監査用証明書送信手段と、前記監査用の要求を前記順次集約木に割り当てた以後に、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第２の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、を有することを特徴とする。

【００２７】

請求項１７記載の本発明は、請求項１６記載の発明において、前記証明書の即時補完情報を含むことを特徴とする。

【００２８】

請求項１８記載の本発明は、請求項１６又は１７記載の発明において、前記監査用証明書作成手段は、さらに、前記利用者装置からの前記要求を前記順次集約木に割り当てた以前に、監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、監査用証明書を作成するとともに、前記監査用の前記要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、該監査用証明書に含める手段を備え、前記一定時間間隔終了後に前記監査用証明書作成手段で作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、を有することを特徴とする。

【００２９】

請求項１９記載の本発明は、請求項１６乃至１８のいずれか1項に記載の発明において、前記順次割当データは、前記要求に含まれるデジタル情報に対して所定の衝突困難一方向関数を適用した結果値であることを特徴とする。

【００３０】

請求項２０記載の本発明は、請求項１６乃至１９のいずれか1項に記載の発明において、前記証明書は、デジタル署名が施されていることを特徴とする。

【００３１】

請求項２１記載の本発明は、請求項１６乃至２０のいずれか1項に記載の発明において、前記一定時間間隔終了後に前記順次集約木のルート値を電子的に公表する電子的情報公表手段を有することを特徴とする。

【００３２】

請求項２２記載の本発明は、請求項16乃至２１のいずれか1項に記載の発明において、前記証明装置は、複数の前記要求を前記順次集約木に順次割り当てたときは、割り当てた時間的順序で、前記複数の要求に対する証明書を送信する手段を有することを特徴とする。

【００３３】

請求項２３記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの該要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記監査装置であって、前記証明装置は、前記利用者装置からの前記要求を受信する順序証明要求受信手段と、前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する

順次割当データ計算手段と、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第１の順次集約木特定情報を含む証明書を作成する証明書作成手段と、前記証明書を前記利用者装置に送信する証明書送信手段と、前記利用者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、複数の監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、前記複数の監査用の前記要求を前記順次集約木に割り当てた時点におけるそれぞれの監査用の前記即時補完情報を前記順次集約木から取得し、前記複数の監査用証明書に含める監査用証明書作成手段と、前記監査用証明書を前記監査装置に送信する監査用証明書送信手段と、前記証明書送信後、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第２の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、を有し、前記証明装置から、前記複数の監査用証明書を受信する監査用証明書受信手段と、前記利用者装置から、前記証明書及び前記遅延補完情報を含む前記証明書に対する監査要求を受信する監査要求受信手段と、受信した複数の監査用証明書の中から、受信した監査要求の第１及び第２の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より生成された時間的順序が後、かつ遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第１の監査用証明書選択手段と、前記順次集約木の特定のノードに対して、前記第１の監査用証明書選択手段で選択された監査用証明書に含まれる該ノードの割当値と、前記監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第１の証明書監査手段と、前記証明書の監査結果を前記利用者装置に送信する監査結果送信手段と、を有することを特徴とする。

【００３４】

請求項２４記載の本発明は、請求項２３記載の発明において、前記監査用証明書受信手段は、前記監査用証明書を受信する第１の時刻を時刻提供装置から取得する手段を有し、前記第１の証明書監査手段は、前記証明書の要求受付が前記第１の時刻よりも時間的に前であることを示す区間時刻証を監査結果に含めることを特徴とする。

【００３５】

請求項２５記載の本発明は、請求項２３又は２４記載の発明において、前記証明装置は、前記一定時間間隔終了後に前記監査用証明書作成手段で作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、を有し、受信した複数の監査用証明書の中から、受信した監査要求の第１の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より時間的順序が前の監査用証明書を選択する第２の監査用証明書選択手段と、前記順次集約木の特定のノードに対して、前記監査要求に含まれる該ノードの割当値と、前記第２の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明す

る第２の証明書監査手段と、を有することを特徴とする。

【００３６】

請求項２６記載の本発明は、請求項２５記載の発明において、複数の証明書に対する各監査結果と、前記複数の証明書の第１の順次集約木特定情報に基づいて、前記複数の証明書間における要求受付の時間的順序を判定する利用者間順序判定手段と、を有し、前記監査結果送信手段は、前記複数の証明書間における要求受付の時間的順序を前記監査結果に含めることを特徴とする。

【００３７】

請求項２７記載の本発明は、請求項２５又は２６記載の発明において、前記監査用証明書及び該監査用証明書の遅延補完情報から前記順次集約木のルート値を計算するルート値計算手段と、電子的に公表された前記順次集約木のルート値と計算されたルート値が一致するか否かの検証を行うルート値検証手段と、を有することを特徴とする。

【００３８】

請求項２８記載の本発明は、請求項２５乃至２７のいずれか１項に記載の発明において、前記第１の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報を前記利用者装置に送信する監査用補完情報送信手段を有することを特徴とする。

【００３９】

請求項２９記載の本発明は、請求項２５乃至２８のいずれか1項に記載の発明において、前記監査用証明書受信手段は、監査用の前記要求を前記証明装置に送信する第２の時刻を時刻提供装置から取得する手段を有し、前記第２の証明書監査手段は、前記証明書の要求受付が前記第２の時刻より時間的に後であることを示す区間時刻証を監査結果に含めることを特徴とする。

【００４０】

請求項３０記載の本発明は、請求項２５乃至２９のいずれか1項に記載の発明において、前記監査結果は、デジタル署名が施されていることを特徴とする。

【００４１】

請求項３１記載の本発明は、請求項１乃至７のいずれか１項に記載のイベント順序証明方法の各ステップを前記証明装置に実行させるイベント順序証明プログラムであることを特徴とする。

【００４２】

請求項３２記載の本発明は、請求項８乃至１５のいずれか１項に記載のイベント順序証明監査方法の各ステップを前記証明監査装置に実行させるイベント順序証明監査プログラムであることを特徴とする。

【００４３】

請求項３３記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの前記要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記利用者装置のためのイベント順序証明検証プログラムであって、前記証明装置は、前記利用者装置からの前記要求を受信する順序証明要求受信手段と、前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに１つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を連接した連接値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第１の順次集約木特定情報を含む証明書を作成する証明書作成手段と、前記証明書を前記利用者装置に送信する証明書送信手段と、前記利用

者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、複数の監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、前記複数の監査用の前記要求を前記順次集約木に割り当てた時点におけるそれぞれの監査用の前記即時補完情報を前記順次集約木から取得し、前記複数の監査用証明書に含める監査用証明書作成手段と、前記監査用証明書を前記監査装置に送信する監査用証明書送信手段と、前記証明書送信後、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第２の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、を有し、前記監査装置は、前記証明装置から、前記複数の監査用証明書を受信する監査用証明書受信手段と、前記利用者装置から、前記証明書及び前記遅延補完情報を含む前記証明書に対する監査要求を受信する監査要求受信手段と、受信した複数の監査用証明書の中から、受信した監査要求の第１及び第２の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より生成された時間的順序が後、かつ遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第１の監査用証明書選択手段と、前記順次集約木の特定のノードに対して、前記第１の監査用証明書選択手段で選択された監査用証明書に含まれる該ノードの割当値と、前記監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第１の証明書監査手段と、前記証明書の監査結果を前記利用者装置に送信する監査結果送信手段と、を有し、前記要求を前記証明装置に送信する順序証明要求送信ステップと、前記証明装置から、前記証明書を受信する証明書受信ステップと、前記証明書の補完情報の要求を前記証明装置に送信する補完情報要求送信ステップと、前記証明装置から、前記補完情報を受信する補完情報受信ステップと、前記監査要求を前記監査装置に送信する監査要求送信ステップと、前記監査結果を受信する監査結果受信ステップと、を前記利用者装置に実行させることを特徴とする。

【００４４】

請求項３４記載の本発明は、請求項３３記載の発明において、前記監査装置の前記監査用証明書受信手段は、前記監査用証明書を受信する第１の時刻を時刻提供装置から取得する手段を有し、前記第１の証明書監査手段は、前記証明書の要求受付が前記第１の時刻よりも時間的に前であることを示す区間時刻証を監査結果に含め、前記要求を前記証明装置に送信する時点の第３の時刻を前記時刻提供装置から取得し、該第３の時刻を所定の手順に従って計算した値を前記要求に含める順序証明要求作成ステップを前記利用者装置に実行させることを特徴とする。

【００４５】

請求項３５記載の本発明は、請求項３３又は３４記載の発明において、前記証明装置は、前記一定時間間隔終了後に前記監査用証明書作成手段で作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、を有し、前記監査装置は、受信した複数の監査用証明書の中から、受信した監査要求の第１の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より時間的順序が前の監査用証明書を選択する第２の監査用証明書選択手段と、前記順次集約木の特定のノードに対して、前記監査要求に含まれる該ノードの割当値と、前記第２の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時

間的前後を証明する第２の証明書監査手段と、を有することを特徴とする。

【００４６】

請求項３６記載の本発明は、請求項３５記載の発明において、前記監査装置は、複数の証明書に対する各監査結果と、前記複数の証明書の第１の順次集約木特定情報に基づいて、前記複数の証明書間における要求受付の時間的順序を判定する利用者間順序判定手段を有し、前記監査結果送信手段は、前記複数の証明書間における要求受付の時間的順序を前記監査結果に含め、前記監査要求は、他の証明書との時間的順序の判定要求を含むことを特徴とする。

【００４７】

請求項３７記載の本発明は、請求項３５記載の発明において、前記監査装置は、前記第１の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報を前記利用者装置に送信する監査用補完情報送信手段を有し、前記監査装置から送信された監査用証明書及び該監査用証明書の遅延補完情報を受信するステップを前記利用者装置に実行させることを特徴とする。

【００４８】

請求項３８記載の本発明は、請求項３４乃至３７のいずれか１項に記載の発明において、前記監査用証明書受信手段は、監査用の前記要求を前記証明装置に送信する第２の時刻を時刻提供装置から取得する手段を有し、第２の証明書監査手段は、前記証明書の要求受付が前記第２の時刻より時間的に後であることを示す区間時刻証を監査結果に含め、前記要求を前記証明装置に送信する時点の第３の時刻を前記時刻提供装置から取得し、該第３の時刻を所定の手順に従って計算した値を前記要求に含める順序証明要求作成ステップを前記利用者装置に実行させることを特徴とする。

【００４９】

請求項３９記載の本発明は、請求項３３乃至３８のいずれか１項に記載の発明において、前記証明装置から受信した証明書、及び前記一定時間間隔終了後に取得した該証明書の補完情報すべてから、前記順次集約木のルート値を計算するルート値計算ステップと、前記一定時間間隔終了後に電子的に公表された前記順次集約木のルート値と計算されたルート値が一致するか否かの検証を行うルート値検証ステップと、を前記利用者装置に実行させることを特徴とする。

【００５０】

請求項４０記載の本発明は、請求項３４又は３８記載のイベント順序証明検証プログラムを実行する利用者装置が前記要求に付した時刻を検証するコンピュータが読み取り可能なイベント時刻検証プログラムであって、前記監査結果を取得する監査結果取得ステップと、前記監査結果に対応する前記要求を取得する順序証明要求取得ステップと、前記第３の時刻と、前記第１又は第２の時刻のうち少なくとも１以上との時間差に基づいて、前記第３の時刻の正当性を判定する時刻検証ステップと、前記判定結果を出力するステップと、

前記コンピュータに実行させることを特徴とする。

【発明の効果】

【００５１】

本発明によれば、木構造を用いてイベント順序を証明するイベント順序証明システムにおいて、イベント順序証明要求をまとめた公表データを用いなくても、イベント順序証明機関から発行されたイベント順序受理証明書の検証を行うことができる。

【００５２】

この結果、公表期間の途中であっても、受け取ったイベント順序受理証明書の正当性を検証することができ、利用者の利便性の向上を図ることができる。また、イベント順序証明機関に障害が発生しても、障害に強いイベント順序証明システムを構築することができる。

【発明を実施するための最良の形態】

【００５３】

以下、本発明の実施の形態を図面を用いて説明する。

【００５４】

＜第１の実施の形態＞

（１－１．システム構成）

図1は、本発明の第１の実施の形態に係るイベント順序証明システム100のシステム構成図である。同図に示すイベント順序証明システム100は、イベント順序証明装置（以下、証明装置という）1、複数のイベント順序証明利用者装置（以下、利用者装置という）2i（i=a, b, …, n）、証明装置1が発行したイベント順序受理証明書（以下、受理証明書という）の監査を行うイベント順序証明監査装置（以下、監査装置という）3、及び、以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成されるコンピュータネットワーク4を備えており、証明装置1が利用者装置2iからのイベント順序証明要求（以下、証明要求という）に応えて、受理証明書を発行し、利用者装置2iに返信すると共に、受理証明書に疑義が生じた場合には、利用者装置2iは、証明装置1が公表したデータ又は監査装置3による監査結果によって受理証明書を検証することができるようになっている。

【００５５】

尚、図１に示すイベント順序証明システム100のシステム構成は機能が同一であればその形態は問わないものであり、その物理的構成は種々考えられるものである。例えば、図２に示すように、利用者装置2iの代わりに、イベント順序証明利用者検証装置（以下、利用者検証装置という）6iが受理証明書の検証を行うようにしてもよいし、証明装置1の代わりに電子的情報公表装置5が証明装置1から公表データをもらい、公開するようにしてもよい。また、コンピュータネットワーク4は、郵便など他の通信手段に置き換えることも可能である。尚、以下においては、図１のシステム構成のもとに構成及び動作を説明する。

【００５６】

証明装置1は、コンピュータネットワーク4を介して利用者装置2i及び監査装置3とデータの送受信を行う送受信部11、利用者装置2iからの証明要求として送信されたデジタル・データを順次集約木を用いてまとめるイベント順序証明要求集約部12、受理証明書を作成するイベント順序証明作成部13、監査装置3に送信する監査情報を作成する監査情報作成部14、利用者装置2iからの補完データ要求に応えて補完データを取得する補完データ取得部15、証明装置1が一定期間に発行した複数の受理証明書の内容を連結したデータに対して高強度デジタル署名をする高強度デジタル署名作成部16、高強度デジタル署名されたデータを電子的に公表する電子的情報公表部17、及び受理証明書をはじめとするイベント順序証明に関する情報を記憶する記憶部１８を有する構成である。

【００５７】

上述したように、イベント順序証明要求集約部12は、順次集約木を用いてイベント順序証明要求をまとめるが、この順次集約木について図3を用いて説明する。図3に示す順次集約木は、一定期間（例えば1週間など証明装置1が取り纏めデータを公表するサイクル、以下、順次集約期間という）において完成される集約木であって、利用者装置2iからの証明要求に含まれるデジタル・データの全部あるいは一部から所定の順次割当データ計算手順に従って生成されたデジタル・データ（これを順次割当データと呼ぶ；例えば、証明要求に含まれるデジタル・データのハッシュ値）を経時的に順次リーフに左側から割り当てるようにしている。

【００５８】

順次集約木の各ノード（リーフを除く）に割り当てられる値の計算方法は、以下の通りである。順次集約木の親の割当値は、左側の子の割当値H'と右側の子の割当値H"を連接（ビット列とビット列の結合）し、所定の衝突困難一方向ハッシュ関数hを適用した結果であるハッシュ値を計算することにより求められるものであり、これをh(H‖H")と表す。このようにして下位のレベルの割当値から上位のレベルの割当値を計算して、最終的に最上位のレベル（ルート）の割当値（ルート値）を求める。

【００５９】

以下においては、図3に示すように、16のリーフを有する順次集約木の場合について説明する。尚、順次集約木リーフの数や高さは、順次集約期間が終了するまで確定しない。また、順次集約木においては、リーフへの値の割当は左から順次行われ、レベルが0より大きいノード（即ちリーフではないノード）に対する値の割当は、それが可能になったときにインクリメンタルに行われる。従って、図3の同一の縦線上にある複数のノードに対しては、値の割当が同一の処理単位の中でほぼ同時に行われる。

ここで、順次集約木のレベルj、番号（インデックスともいう）iのノードを（j，i）で表し、ノード（j，i）の割当値をV(j，i)と表して、図3に示す具体例を説明する。

【００６０】

今、順次割当データがノード(0,5)に割り当てられたとき、即ち、順次集約木リーフに割り当てるハッシュ値がV(0,5)であるとき、このハッシュ値V(0,5)からルート値（＝V(4,0)）を求めるには、V(0,5)にV(0,4)を左から連接して、ハッシュ値h1'を計算し、該ハッシュ値h1'にV(1,3)を右側から連接してハッシュ値h2'を計算し、該ハッシュ値h2'にV(2,0)を左側から連接してハッシュ値h3'を計算し、さらに該ハッシュ値h3'にV(3,1)を右側から連接してハッシュ値（＝V(4，0)）を計算すればよい。このような手順によりV(0，5)とそれを補完するデータ（ここではV(0，4)，V(1,3)，V(2,0)，V(3,1)）からルート値が計算できるとき、V(0，5)はハッシュ関数hによりルート値にリンクするという。また、順次集約木におけるV(0,5)の補完データ（以下、順次集約補完データという）は、

［（V(0,4)，L）、（V(1,3)，R）、（V(2,0)，L）、（V(3,1)，R）］

となる。ここで、L 及び R は、各々、２つのデジタル・データを連接する際に左から連接こと、及び右から連接することを表す。

【００６１】

イベント順序証明作成部13は、図４に示すような受理証明書 EOC(y)を作成し、利用者装置2iに送信するようになっている。同図によれば、受理証明書 EOC(y)は、利用者から送付されたデジタル・データy、上述した順次割当データ計算手順によりデジタル・データyから計算された順次割当データz、順次割当データzが割当てられた順次集約木を一意に特定できる順次集約木番号、順次割当データzが割当てられた順次集約木リーフを一意に特定できる順次集約木リーフ番号、およびその時点で取得できる順次集約補完データの一部（これを即時補完データという） HK を含むように構成されている。このうち、即時補完データHKについては省くことも可能である。

【００６２】

また、同図によれば、イベント受理証明書 EOC(y) には、証明装置1が予め用意しておいた公開鍵暗号方式キー・ペアのうちの秘密鍵（署名用秘密鍵）を用いてデジタル署名をつけて送信してもよい。この場合、当該公開鍵暗号方式キー・ペアのうちの公開鍵は公開鍵暗号基盤などを用いて利用者装置2iからアクセス可能になっているものとする。

【００６３】

尚、当該の受理証明書EOC(y)発行後に取得できる順次集約補完データを遅延補完データという。即ち、受理証明書 EOC(y) が作成される段階においては、即時補完データだけが利用者装置2iに送信されるものであり、遅延補完データは、当該の受理証明書EOC(y)発行後に要求された場合等に利用者装置2iに送信されるものである。例えば、図3の具体例においては、ノード(0,5)にとって、ノード割当値V(2,0)、ノード割当値V (0,4)は即時補完データであるが、ノード割当値V (1,3)、ノード割当値V (3,1)はノード(0，15)が割当られた時点以降に取得可能な遅延補完データである。以下では、順次集約木リーフ番号 i に対して、V(0，i) のことを短く V(i) と書くこともある。

【００６４】

補完データ取得部14は、利用者装置2iから上述した遅延補完データの要求があったとき、当該時点に関する情報（当該要求が割り当てられた順次集約木番号、順次集約木リーフ番号）、及びその時点で確定している順次集約補完データ（位置情報、割当値）の全てを利用者装置2iに返送するようになっている。

【００６５】
ここで、図５を参照して、順次集約補完データの内容について詳しく説明する。
【００６６】
順次集約木の１つのリーフ tに対する、t より右に位置するもう一つのリーフt'における補完データ CToken(t, t') は次のように定義される。
【００６７】
リーフtから順次集約木のルートに至るパスをtのルート・パスと呼び、tのルート・パスに属するルート以外のノードの兄弟ノードからなるノードの並びをtの認証パスと呼ぶ（認証パスの詳細な定義は後で与える）。 認証パスの要素の内、tより右に位置するリーフt1の割り当て値が確定した時点において割当値が確定している要素の列を authPathD(t, t1) とし、これを t1におけるtに対する認証パスと呼ぶ。この列に割当値の情報を付加したものを authPathDV(t, t1) とし、これを t1におけるtに対する値付認証パスと呼ぶ。
【００６８】
以上から、authPathDV(t, t') は、受理証明書EOC(y) に含まれていなかった情報を含めて、補完データCToken(t, t') を構成するようになっている。
【００６９】
尚、t' が t の属する順次集約木 SBT の生成期間（順次集約期間）の終了後に生成される次の順次集約木SBT'のリーフであるときにも、authPathDV(t, t') には順次集約木SBT についての情報のみが含まれる。このとき、CToken(t, t') は、t 時点で受信したイベント受理証明書EOC(y)と組み合わせることにより、当該の順次集約期間における順次集約木のルート値を計算するのに十分な情報をふくんでいる。
【００７０】
例えば、図５において、CToken(t, t4') は a1 の位置情報 (0, 3) とその割当値 V(a1) の組 ((0, 3), V(a1)) 、及びa2 の位置情報 (2, 1) とその割当値 V(a2) の組 ((2, 1), V(a2))
からなる列 [((0, 3), V(a1)), ((2, 1), V(a2))] となる。
【００７１】
以下では、受理証明書に含まれる順次集約木の割当て値と組み合わせることにより前記順次集約木のルート値を計算できるような補完データを該受理証明書の完全補完データと定義し、上記割当て値および受理証明書に含まれる即時の補完データと組みあわせることにより、前記順次集約木のルート値を計算できるような補完データを完全遅延補完データと呼ぶ。
【００７２】
監査情報作成部14は、監査情報を順次集約木から取得して監査装置3に送信するものであり、より詳しくは、監査情報とは、順次集約木リーフに設けられた監査点において以下に定義するように生成される監査用イベント順序受理証明書（以下、監査用受理証明書という）から構成される。ここで、監査点とは、監査装置3からの監査用イベント順序証明要求（以下、監査用証明要求という）が割当てられた順次集約二分木のリーフをいう。
【００７３】
尚、図3の具体例においては、監査点は1つしか設けられていないが、所定のアルゴリズムに従って複数設けてよいのは勿論であり、また、証明要求に対する受理証明書に対して後述するような監査を行うためには、監査点は、該証明要求に対応するリーフ（図3の具体例においては、ノード(0, 5)）に等しいか或いはそれより右側のリーフ（時間的に後）に割り当てられていればとこに設けていてもよいものである。
【００７４】
監査用受理証明書の形式は、利用者装置2iに返送する受理証明書と同一である。尚、順次割当データを計算するための元となるデジタル・データyは、監査装置3から証明装置1に監査用証明要求として送付されたものであってもよいし、当該証明装置1において、当該の監査装置2に対して予め定められた何らかの手順に従って生成してもよい。また、こ

のような手順としては、前以て定められた何らかの手順に従って監査用受理証明書におけるイベント順序証明の対象となるデジタル文書を作成し、該デジタル文書に対して前以て定めたハッシュ関数を適用した結果であるハッシュ値を順次割当データを計算するための元となるデジタル・データとする方式を採用してもよい。

【００７５】

利用者装置2iは、コンピュータネットワーク4を介して証明装置1および監査装置3とデータを送受信する送受信部21、所定のデジタル・データを含む証明要求を行うイベント順序証明要求部22、要求時点において取得可能な受理証明書に対する補完データを要求する補完データ要求部23、受理証明書を検証するイベント順序証明検証部24、受理証明書をはじめとするイベント順序証明に関する情報を記憶する記憶部25を有する構成である。

【００７６】

ここで、イベント順序証明検証部24は、受理証明書に対して以下の検証機能を備える。

【００７７】

まず、受理証明書にデジタル署名が含まれる場合には、該デジタル署名に対するデジタル署名検証を行う第０の検証機能を備える。

【００７８】

また、証明装置1から高強度デジタル署名を付すこと等により真正性を保証して公表される公表情報に、受理証明書に含まれる順次割当データがハッシュ関数を介してリンクすることを検証する第１の検証機能を備える。

【００７９】

さらに、以下に記述するように、証明装置1からの公表情報が公開される前であっても、監査装置3を利用することにより、受理証明書の正当性を検証する第２の検証機能を備える。

【００８０】

監査装置3は、コンピュータネットワーク4を介して証明装置1および利用者装置2iとデータを送受信する送受信部31、利用者装置2iからある受理証明書の監査要求を受けた際には、利用者装置2iから送信された監査要求情報および自己の監査情報を用いて受理証明書の検証を行い、その結果を利用者装置2iに返信するイベント順序証明監査部32、及び監査用受理証明書をはじめとする監査情報を記憶する記憶部33を有する構成である。

【００８１】

ここで、イベント順序証明検証部32の機能について、図3の具体例を用いて説明する。図3の具体例においては、(0,10) が監査点となっているので、この時点において監査装置3が受け取っている監査情報は、上述した通り、V(3,0)およびV(1,4)である。一方、利用者装置2iは、監査要求情報として、V(0, 5) 及び順次集約補完データであるV(0,4)、V(1,3)、およびV(2,0)を送信するものである。これは、利用者装置2iが検証を求める時点（即ち、受理証明書が発行された(0,5)の時点より後刻である監査点(0,10)の時点以降）においては、即時補完データに含まれていなかったV(1,3)も証明装置1から取得することが可能であるので、V(1,3) を遅延補完データとして利用者装置2iが証明装置1から取得し、監査要求情報に含めたものである。そして、イベント順序証明検証部32は、自己が有している監査情報 V(3,0) が、利用者装置2_jから送信された監査要求情報から計算された V(3,0) と一致するか否かを検証するものである。

【００８２】

尚、以後においては、利用者装置2iから送信された証明要求から作成された順次割当データが割り当てられた順次集約木リーフをユーザ点と呼び、監査装置3から送信された監査用証明要求から作成された順次割当データが割り当てられた順次集約木リーフを監査点と呼ぶ。

【００８３】

ここで、比較検証の対象となる順次集約木のノード（図3の具体例においては、(3,0)）を以後、認証点とよぶ。尚、一般に、あるユーザ点の番号が監査点の番号より小さい場合、認証点のラベル（割当値）は監査情報に含まれており、また、監査点におけるイベント

順序証明処理が終了した時点以降において、利用者装置2iが受信できる遅延補完データから計算できるラベルには、認証点のラベルが含まれるので、順次集約木においてユーザ点、監査点、遅延補完データを要求した点が左からこの順序に位置している場合には、上記検証は、常に実施可能なものであるが、この理由に関しては後述する(後述の順次集約木の性質2の項目(3)を参照)。

【００８４】

即ち、上記の手順により利用者装置2iがある受理証明書に対する第２の検証を監査装置3に依頼して実行するには、該受理証明書の証明要求が割り当てられたリーフτと、該イベント受理証明書に対する遅延補完データ要求が割り当てられたリーフτ'の間(τとτ'も含む)に監査装置3の監査点が存在する必要がある。

【００８５】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置（CPU：Central Processing Unit）、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置（メモリ）、ハードディスク（HD）等の電源断時にもデータを記憶し続けることが出来る２次記憶装置を有する電子的な装置から構成されている。このうち、証明装置1のイベント順序証明要求集約部12、イベント順序証明作成部13、監査情報作成部14、補完データ取得部15、デジタル署名作成部16及び電子的情報公表部17、利用者装置2iのイベント順序証明要求部22、補完データ要求部23及びイベント順序証明検証部24、並びに監査装置3のイベント順序証明監査部32の処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、証明装置1の記憶部18、利用者装置2iの記憶部25及び監査装置3の記憶部33は、上記主記憶装置あるいは２次記憶装置の機能を備えたものである。

【００８６】

また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置または２次記憶装置に格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ－ＲＯＭなどのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

【００８７】

（１－２．システム動作）

次に、以上の構成を有するイベント順序証明システム100におけるイベント順序証明方法、およびイベント順序証明検証方法を図６乃至８を用いて説明する。ここで、図６は、１つの順次集約期間において証明装置1が受理証明書及び監査用受理証明書を作成する動作を説明するシーケンス図であり、図７は、利用者装置2iが受理証明書に対して第1の検証を行う動作を説明するフローチャートであり、図８は、利用者装置2iが受理証明書に対して第２の検証を行う動作を説明するシーケンス図である。

【００８８】

まず、図６を参照して、イベント順序証明方法について説明する。

【００８９】

利用者装置2iが証明装置1にデジタル・データｙを含む証明要求を送信すると、証明装置1は送受信部11を介して、該デジタル・データｙを含む証明要求を受信する(ステップＳ10、Ｓ20)。

次に、イベント順序証明要求集約部12が、デジタル・データｙを入力の一部あるいは全部として順次割当データｚを計算し、該順次割当データｚを順次集約木リーフに割り当て、インクリメンタルに順次集約木を構成していくとともに、イベント順序証明作成部13が、受理証明書EOC(y)を作成し、送受信部11を介して利用者装置2iに受理証明書EOC(y)を送信する（ステップＳ30、Ｓ40、Ｓ50）。

【００９０】

これにより、利用者装置2iは、受理証明書 EOC(y) を取得することができる（ステップＳ60）。尚、受理証明書 EOC(y) には、この時点において取得できる即時補完データを含

めることにしてよいが、遅延補完データは含まれていない。

【００９１】

同様にして、監査装置３も監査用証明要求を送信すると、証明装置1は送受信部11を介して、監査用証明要求を受信する(ステップＳ70、Ｓ80)。

【００９２】

次に、イベント順序証明要求集約部12が、監査用証明要求から計算された監査用順次割当データを順次集約木リーフに割り当てて、インクリメンタルに順次集約木を構成していくとともに、監査情報作成部13は、監査用受理証明書を作成し、送受信部11を介して監査装置3に監査用受理証明書を送信する（ステップＳ90、Ｓ100、Ｓ110）。

【００９３】

これにより、監査装置3は、監査用受理証明書を取得することができる（ステップＳ120）。

【００９４】

次に、利用者装置2iは、取得した受理証明に対する遅延補完データ要求を証明装置1に送信すると、証明装置1は送受信部11を介して、該遅延補完データ要求を受信する(ステップＳ130、Ｓ140)。

【００９５】

次いで、証明装置1の補完データ取得部15は、その時点で取得可能な上記受理証明書に対する補完データを取得し、遅延補完データとして送受信部11を介して利用者装置2iに送信する（ステップＳ150、Ｓ160）。

【００９６】

これにより、利用者装置2iは、監査に必要な遅延補完データを取得することができる（ステップＳ170）。

【００９７】

そして、順次集約のための一定期間（順次集約期間）内においては、上述した証明装置1の動作は繰り返され、順次集約期間が終了すると、順次集約木のルート値 を計算し、電子的情報公表部17は、このルート値を電子的に公表する（ステップＳ180、Ｓ190、Ｓ200）。この際、該情報の真正性を保証するため、高強度デジタル署名作成部 16を用いて高強度のデジタル署名を付した公表情報を公開してもよい。

【００９８】

尚、図６に示すイベント順序証明方法においては、監査装置3の方から証明装置１に監査情報要求を送信し、これに応えて証明装置１が監査装置3に監査情報を送信する方式であったが、これとは異なり、証明装置１が監査装置3に監査情報を自動的に送信するような方式であってもよい。

【００９９】

次に、図７を参照しながら、電子的に公表された公表情報を用いたイベント順序証明検証方法について説明する。これは、利用者装置2iの第１の検証機能に相当するものである。

【０１００】

まず、利用者装置2_iは、自己が証明装置1に証明要求として送信したデジタル・データy、並びに受信した受理証明書 EOC(y) 及び遅延補完データに含まれている順次集約補完データ（この時点においては、すべての順次集約補完データを取得可能である）から順次集約木のルート値 RH_{cal} を計算する（ステップＳ310）。

次に、高強度のデジタル署名を付して電子的に公表されている同一順次集約期間のルート値RHを取得し、このルート値RHが、計算したルート値RH_{cal} に一致するか否か検証する（ステップＳ320、Ｓ330）。

【０１０１】

以上の検証において、検証に成功すれば、受理証明書が改ざんされていないことを確認することができる（ステップＳ340）。一方、検証に失敗すれば、受理証明書が改ざんされていることを確認することができる（ステップＳ350）。これにより、高強度のデジタ

ル署名を付すなどの手段により真正性を保証しながらが電子的に公表された後においては、公表された情報を利用して、証明装置1が発行した受理証明書が、当該の順次集約期間において、受理証明書に含まれる元デジタル・データに対して、受理証明書に含まれる順次集約木リーフ番号で識別される順番において発行されたものであることを確実に検証することができる。

【０１０２】

次に、図８を参照しながら、監査装置3を用いたイベント順序証明検証方法について説明する。これは、利用者装置2iの第２の検証機能に相当するものである。

【０１０３】

利用者装置2iは、監査要求の前に検証の対象となる受理証明書の遅延補完データを証明装置1に要求する（ステップＳ410）。この要求を証明装置1が送受信部11を介して受信すると、補完データ取得部15は、受理証明書に即時補完データが含まれる場合には、この時点において取得できる遅延補完データの全てから即時補完データを除いたものからなる遅延補完データを、受理証明書に即時補完データが含まれない場合には、この時点において取得できる遅延補完データの全てを取得し、送受信部11を介して利用者装置2iに送信する（ステップＳ420、Ｓ430、Ｓ440）。これにより、利用者装置2iは、補完データを取得するので、イベント順序証明検証部24は、これに既に受け取っている受理証明書を加えた監査要求情報を監査装置3に送信する（ステップＳ450、Ｓ460）。

【０１０４】

次に、監査装置3が監査要求情報を送受信部31を介して受信すると、イベント順序証明監査部32は、既に自分が受信した監査用受理証明書が割当てられた順次集約木のリーフの中で、受信したこの監査要求情報に含まれる受理証明書が割当てられた順次集約木リーフτとその遅延補完情報に含まれるリーフτ'の間にある監査点αを計算する（ステップS470、S480）。続いて、監査要求情報からτのαによる認証点を計算し、該認証点の割当値A_{cal}を計算する（ステップＳ490）。一方、イベント順序証明検証部32は、監査情報として既に受け取っているこの認証点の割当値Ａを記憶部33から取得して、この認証点の割当値Ａが、計算により求めた認証点の割当値A_{cal}に一致するか否かを検証する（ステップＳ500、Ｓ510）。

以上の検証において、検証に成功すれば、受理証明書が改ざんされていないことを確認することができる（ステップＳ520）。一方、検証に失敗すれば、受理証明書が改ざんされていることを確認することができる（ステップＳ530）。そして、イベント順序証明監査部32は、この監査結果を送受部31を介して利用者装置2iに送信し、利用者装置2iは、監査結果を受信する（ステップS540、Ｓ550）。

【０１０５】

これにより、利用者装置2iは、電子的公表機関を介した公表前においても、証明装置1が発行した受理証明書が当該の順次集約期間において、受理証明書に含まれる元デジタル・データに対して、受理証明書に含まれる順次集約木リーフ番号で識別される順番において発行されたものであることを確実に検証することができる。尚、上記監査結果に監査点αの識別子を含めてもよい。この場合においては、利用者装置2iは、上記監査を要求した受理証明書に対応する証明要求の登録が、監査点αに対応する監査用証明要求の登録より前であったことの保証を監査装置３から確実に得ることができる。

【０１０６】

なお、ステップＳ540の監査結果の送信に際しては、監査装置3が受信した補完データを含む部分に対して、証明監査装置3が持つ署名用秘密鍵を用いてデジタル署名を付して、該デジタル署名を含めた検証結果を構成し、利用者装置2iに送信するようにしてもよい。これにより、監査装置3によるデジタル署名が信用されるという前提の下で、順次集約木のルート値に対する有効なデジタル署名が入手できない場合であっても、利用者装置2iを利用する利用者は、上記受理証明書によるイベント順序証明の正当性を客観的に第三者に証明することができるようになる。

【０１０７】

（１－３．イベント順序監査方法）

次に、上述した第２の検証である監査装置3を用いたイベント順序証明検証方法について、より詳しく説明する。

【０１０８】

尚、以下では、時刻の原点として、イベント順序証明システム100のサービス開始時点をとり、時間を計る単位として一つの値（例えば１秒、１ミリ秒等）を定め、時刻を上記原点から上記の時間の単位で計った整数で表現するものとする。

【０１０９】

また、イベント順序証明検証方法を説明するための幾つかの予備定義を与える。

【０１１０】

順次集約木SBTにおいて、1つのノードp はレベルj とレベル内の番号i で識別されるが、ノードp のレベルと番号を各々 level(p)、 index(p) と書く。

【０１１１】

また、順次集約木リーフ番号i で識別される順次集約木SBTのリーフをleaf(SBT, i) 、leaf(SBT, i) に順次割当値を割り当てる元となった証明要求を受付けて該リーフに割当値を割り当てる一連の処理を該リーフに対する処理ラウンドと言いround(SBT, i) と表す。文脈からとの順次集約木について論じているか明らかなときは、単に leaf(i)、 round(i)と記すこともある。

【０１１２】

順次集約木には、生成された順に0 から始まる識別番号を付与し、これを順次集約木番号という。n番目の順次集約木リーフの数をN(n)とおく。

【０１１３】

各受理証明書に対しては、順次集約木番号nと順次集約木リーフ番号iが付与され、該受理証明書が発行された順次集約木リーフをそれら２つの番号の組で指定することができる。このような組を拡張リーフ識別子と呼ぶ。２つの拡張リーフ識別子 $\nu 1 = (n1, i1)$、$\nu 2 = (n2, i2)$ の間の順序を辞書式順序を用いて定義する。即ち、$\nu 1 < \nu 2$ とは、n1 < n2、またはn1＝n2 かつ i1 < i2 のことと定義する。また$\nu 1 \leqq \nu 2$とは、$\nu 1 < \nu 2$または$\nu 1 = \nu 2$のことと定義する。$\nu = (n, i)$ を拡張リーフ識別子とし、この識別子で識別される順次集約木リーフがあるとき、該リーフを leaf(ν) ＝leaf(n, i)と表す。leaf(ν)を単に、リーフνと呼ぶこともあり、leaf(ν)が監査点（あるいはユーザ点）であるときは、監査点ν（あるいはユーザ点ν）と呼ぶこともある。

【０１１４】

また、ある順次集約木SBTのリーフ leaf(SBT, i) について、この順次集約木SBTのリーフに順次割当値を割り当てる元となった証明要求の受付時刻を、該リーフに対応する時刻といい、これをtime(SBT, i) あるいは簡単にtime(i) と表す。同様に、leaf(ν)について、このリーフに順次割当値を割り当てる元となった証明要求の受付時刻を、time(ν)と表す。

【０１１５】

利用者装置2iが、監査装置3を用いて、ある受理証明書に対する第２の検証を実行するには、上述したように該受理証明書に対応する順次集約木リーフτと、該受理証明書に対する遅延補完データ要求に対応する順次集約木リーフ τ' の間(τ とτ' も含む)に監査装置3の監査点αが存在する必要がある。このためには、Tをある正整数とし、以下の３つの条件（１）、（２）、（３） が成り立てば十分である。

【０１１６】

（１）監査装置3の最初の監査点の時刻はTより小さい。

【０１１７】

（２）監査装置3による任意の１つの監査点をα、次の監査点をα'とすると、

time(α') － time(α) ≦ Tが成り立つ。

【０１１８】

（３） 利用者装置2i は、拡張リーフ識別子τの順次集約木リーフで受理証明書を受信し

た後のある順次集約木リーフτ'で該受理証明書に対する遅延補完データを受信することとし、

time(τ') − time(τ) ≧ Tが成り立つ。

【０１１９】

尚、これらの条件の十分性の理由に関しては後述する(後述の次集約木の性質3の(1)と(2)を参照)。

【０１２０】

図９に示すようなある順次集約木SBTに属する監査装置3の監査点αにおいて、監査装置3は監査用受理証明書を受信するものとする。監査用受理証明書には、αにおける即時補完データが含まれている。この即時補完データには、順次集約木SBTの任意のリーフτでα より左にあるものの割当値 V(τ)が次のような意味で結合している。即ち、τのαによる認証点p2の割当値V(p2)が上記の即時補完データに含まれ、この認証点の割当値はV(τ)から出発してauthPath(τ)に属する幾つかのノードの割当値をハッシュ関数hによりリンクすることにより計算できる（これが成立つ理由については、後述の順次集約木の性質２の項目(1)を参照）。

【０１２１】

これにより、監査装置3は監査点αで受信した監査用受理証明書内の即時補完データに、上記V(p2)が含まれているか否かにより、利用者がユーザ点τで取得した受理証明書の元となった要求の送信及び証明装置1による要求受付けが、監査装置3が監査点αで取得した監査用受理証明書の受信より時間的に前であることを検証することができる（これを検証結果１とする。図10を参照）。

ここで、証明装置1の直列化可能性について説明する。証明装置1の直列化可能性とは、該証明装置が任意の複数の順序証明要求を受付け処理する際に、該複数の要求を直列に並べるある順序付けがあり、その順序に従って順次受けて、それに対する処理結果である受理証明書を返信し、その後次の要求の処理を行った場合と同じ結果となることと定義する。

【０１２２】

証明装置の直列化可能性は重要な要件であり、本実施の形態においては、直列化可能性を保証する手段を有するものとする。このような手段としては、証明装置が1つ順序証明要求を受付けたとき、該要求に対する受理証明を送信してからのみ次の要求受付けることを監視する直列性監査装置を用いてもよい。

【０１２３】

この直列化可能性を用いれば、ユーザ点と監査点の順序関係について検証結果１より強いことを結論することができる。例えば、順序証明装置1の直列化可能性が、監査装置3が監査点αで取得した受理証明書の受信時まで保証されていたとすると、上記検証により、ユーザ点τに対応する順序証明要求の受付けが、監査点αに対応する監査用順序証明要求の受付けより時間的に前であることを結論できる.（これを検証結果２とする。図10を参照）。なぜならば、直列化された順序証明要求の処理において、αに対応する監査用順序証明要求の受付けがτに対応する監査用順序証明要求の受付けより前であれば、αに対応する受理証明書EOC(α)は、τに対応する監査用順序証明要求 EOR(τ)の受付けより前に送信されることになり、EOC(α) にEOR(τ) が含むイベント値がハッシュ関数を介して結合するデータを含めることは出来ないからである。以上から、監査装置3が監査点αで取得した監査用受理証明書の受信時まで、証明装置1の直列化可能性が推認されるときには、ユーザ点τに対応する順序証明要求の受付けは、監査点αに対応する監査用順序証明要求の受付けより時間的に前であることが推認される。以後、このことを「ユーザ点の未来側の境界付け」という。

【０１２４】

尚、監査装置3が監査点αで取得した監査用受理証明書の受信時までの証明装置1の直列化可能性を保証しても、監査装置3が受理証明の一部として即時補完データを受信していなければ、上記のことは言えないことに注意する必要がある。なぜならば、監査装置3が

監査点αで取得した監査用受理証明書の受信時より後に、証明装置がτにおける割当て値を改変する可能性を除くことはできないからである。

【０１２５】

従って、第１の実施の形態のイベント順序証明システム100によれば、利用者装置2iから証明要求を受付けた証明装置1が、該要求に含まれるデジタル・データから計算される順次割当値及び前記順次割当データが割り当てられた順次集約木の位置情報を含む受理証明書及び補完データを発行し、補完情報順次集約木のルート値に対して高強度デジタル署名を付す等の手段により真正性を保証しながら電子的に公表するので、利用者装置2iは公表情報および補完データから簡単に受理証明書の検証をすることができる。また、順次集約木のルート値を電子的にに公表する前であっても、監査装置3が順次集約木の監査点に関する監査情報を有しているので、監査装置5は利用者装置2iからの監査要求を受けて、受理証明書の監査をすることができる。

【０１２６】

この結果、受理証明書の正当性を検証できたときには、証明装置1における監査対象とした受理証明書の証明要求受信が、監査に用いた監査用受理証明書の証明要求受信よりも時間的に前であることを証明することができる。

【０１２７】

＜第２の実施の形態＞

（２－１．システム構成）

図11は、本発明の第２の実施の形態に係るイベント順序証明システム200のシステム構成図である。同図に示すイベント順序証明システム200は、イベント順序証明装置（以下、証明装置という）7、複数のイベント順序証明利用者装置（以下、利用者装置という）2i（i=a, b, …, n）、証明装置7が発行したイベント順序受理証明書（以下、受理証明書という）の監査を行うイベント順序証明監査装置（以下、監査装置という）8、及び、以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成されるコンピュータネットワーク4を備えており、証明装置7が利用者装置2iからのイベント順序証明要求（以下、証明要求という）に応えて、受理証明書を発行し、利用者装置2iに返信すると共に、受理証明書に疑義が生じた場合には、利用者装置2iは、証明装置7が公表したデータ又は監査装置8による監査結果によって受理証明書を検証することができるようになっている。

【０１２８】

ここで、第２の実施の形態は、第１の実施の形態とほぼ同様のシステム構成であるが、監査装置8が、各順次集約期間の終了後に、その順次集約期間中に取得した各監査用受理証明書の完全遅延補完データを、証明装置7に要求して（あるいは事前の契約に基づいて）取得するという点が異なっている。尚、本実施の形態においては、第１の実施の形態と異なる構成及び機能を説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

【０１２９】

また、第１の実施の形態と同様に第２の実施形態においても、イベント順序証明システム200のシステム構成は機能が同一であればその形態は問わないものであり、その物理的構成は種々考えられるものである。例えば、利用者装置2iの代わりに、利用者検証装置6iが受理証明書の検証を行うようにしてもよいし、証明装置7の代わりに、電子的情報公表装置5が証明装置7から公表データをもらい、公開するようにしてもよい。また、コンピュータネットワーク4は、郵便など他の通信手段に置き換えることも可能である。

【０１３０】

証明装置7は、コンピュータネットワーク4を介して利用者装置2i及び監査装置8とデータの送受信を行う送受信部11、利用者装置2iからの証明要求として送信されたデジタル・データを順次集約木を用いてまとめるイベント順序証明要求集約部12、受理証明書を作成するイベント順序証明作成部13、監査装置8に送信する監査情報を作成する監査情報作成部71、利用者装置2iからの補完データ要求に応えて補完データを取得する補完データ取得

部15、証明装置7が一定期間に発行した複数の受理証明書の内容を連結したデータに対して高強度デジタル署名をする高強度デジタル署名作成部16、高強度デジタル署名されたデータを電子的に公表する電子的情報公表部17、及び受理証明書をはじめとするイベント順序証明に関する情報を記憶する記憶部72を有する構成である。

【０１３１】

監査情報作成部71は、各監査点における監査用受理証明書を順次集約木から取得して作成することに加えて、各順次集約期間の終了後に、その順次集約期間に取得した各監査用受理証明書の完全遅延補完データを取得して作成するようになっている。

【０１３２】

監査装置8は、コンピュータネットワーク4を介して証明装置7および利用者装置2iとデータを送受信する送受信部31、証明装置7に各監査用受理証明書の完全遅延補完データの要求を行う補完データ要求部81、利用者装置2iからある受理証明書の監査要求を受けた際には、利用者装置2iから送信された監査要求情報及び監査情報（監査用受理証明書に加えて該監査用受理証明書の完全遅延補完データも含める）を用いて受理証明書の検証を行い、その結果を利用者装置2iに返信するイベント順序証明監査部82、及び監査用受理証明書をはじめとする監査情報を記憶する記憶部83を有する構成である。

【０１３３】

イベント順序証明監査部82は、第１の実施の形態のイベント順序証明監査部32の機能（「ユーザ点の未来側の境界付け」）に加えて、後述する「ユーザ点の過去側の境界付け」を検証できる機能を有するようになっている。これは、あるユーザ点がある監査点よりも左にあること（即ち、時間的に前にあること）に加えて、あるユーザ点がある監査点より右にあること（即ち、時間的に後であること）を監査できることを意味する。

【０１３４】

以下、図12を参照しながら、この「ユーザ点の過去側の境界付け」について　説明する。

【０１３５】

尚、以下では、監査装置8が各順次集約期間の終了後に、その順次集約期間に取得した各監査用受理証明書の完全遅延補完データを取得することを、監査装置8は複合完全補完を行うという。

【０１３６】

本実施の形態においては、監査装置8は、順次集約期間が終わることに、該順次集約期間に受信した監査用受理証明書に対する完全遅延補完データを取得するので、監査用受理証明書に含まれる即時補完データと該遅延補完データを組み合わせることにより、監査装置8は、該順次集約期間に受信した監査用イベント受理証明書に対する完全補完データを取得することになる。

【０１３７】

ここで、利用者装置2iと監査装置8は、第１の実施の形態で述べた条件（１）（２）及び（３）を満たすものとする。τを利用者装置2iによるユーザ点で、T≦time(τ)を満たすものとする。T≦time(τ)という条件から、上述の条件（１）によりτより左にある（即ち時間的に前にある）監査装置8による監査点が存在する。そのような監査点の一つをα１とおく。α１として、上記条件を満たす監査点のうち最も右に位置するものをとることにしてもよい。監査は以下の手順に従って実行される。

【０１３８】

（１）　利用者装置2iがユーザ点τで取得した受理証明書（順次集約木リーフ番号、即時補完データ）を監査装置8に送付する。

【０１３９】

（２）　監査装置8は利用者装置2iから送付された受理証明書に含まれる順次集約木リーフ番号を取り出し、該受理証明書に対応する順次集約木リーフτを特定し、自分が取得した監査用受理証明書の中から、τより左に位置する順次集約木リーフに対応するものを選ぶ。このような監査用受理証明書の中から、対応する順次集約木リーフがもっとも右に位置

するものを選んでもよい。このように選ばれた監査用受理証明書に対応する順次集約木リーフをα1とする。

【０１４０】

（３） 監査装置8は複合完全補完を行うので、監査装置8は監査点α1に対応する監査用受理証明書の完全遅延補完データを取得する。該遅延補完データに対応する順次集約木リーフは、τと等しいか右に位置する（時間的に後である）。

【０１４１】

（４）監査装置8は、監査点α1に対応する監査用受理証明書とそれに対する上記遅延補完データから、監査点α１のユーザ点τによる認証点ｐ２の割当値を計算することができる。

【０１４２】

（５） 従って、監査装置8は、利用者装置2iから受信した順次集約木リーフτに対応する受理証明書内の即時補完データに、上記計算した監査点α１のユーザ点τによる認証点の割当値が含まれることを検証することにより、α１がτより左に位置することを監査することができる。

【０１４３】

この検証結果からまず言えることは、監査点α1に対応する監査装置7の監査用証明要求が証明装置7に受信された時刻をt1、τに対応する利用者装置2iの証明要求が証明装置7に受信された時刻をt2、この要求に対する受理証明書が証明装置7から送信された時刻をt2'とおくと、t1 < t2'ということである。

【０１４４】

ここで、本実施の形態においても、証明装置7の直列化可能性は保証されている、即ち、t2'の時点まで証明装置7の直列化可能性は保証されているとすると、さらに、t1<t2ということも結論できる。以上から、証明装置7がユーザ点τに対応する受理証明書を利用者装置2iに送信した時刻まで、証明装置7の直列化可能性が推認されるときには、監査点α1に対応する監査用証明要求の受付けは、ユーザ点τに対応する利用者装置2iの証明要求の受付けより時間的に前であることが推認される。

【０１４５】

尚、t2'時点までの証明装置1の直列化可能性を保証しても、利用者装置2iが受理証明の一部として即時補完データを受信していなければ、上記のことは言えないことに注意する必要がある。なぜならば、t2'時点より後で、証明装置7が監査点α1における割当て値を改変する可能性を除くことはできないからである。

【０１４６】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置（CPU：Central Processing Unit）、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置（メモリ）、ハードディスク（HD）等の電源断時にもデータを記憶し続けることが出来る２次記憶装置を有する電子的な装置から構成されている。このうち、証明装置7の監査情報作成部71、並びに監査装置8の補完データ要求部81及びイベント順序証明監査部82の処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、証明装置7の記憶部72及び監査装置8の記憶部83は、上記主記憶装置あるいは２次記憶装置の機能を備えたものである。

【０１４７】

また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置または２次記憶装置に格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ－ＲＯＭなどのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

【０１４８】

（２－２．システム動作）

次に、以上の構成を有するイベント順序証明システム200におけるイベント順序証明方

法、およびイベント順序証明検証方法を図13及び図14を用いて説明する。ここで、図13は、１つの順次集約期間において証明装置7がイベント受理証明書及び監査用受理証明書を作成する動作を説明するシーケンス図であり、図14は、利用者装置2iがイベント受理証明書に対して第２の検証を行う動作を説明するシーケンス図である。

【０１４９】

まず、図13に示すイベント順序証明方法について説明する。尚、本実施の形態に係るイベント順序証明方法において、その動作のほとんとは第１の実施の形態と同様であり、図６のステップＳ10～Ｓ200は、図13のステップS610～S800と同一で、その後のステップS810～S850が新たに追加されたものである。従って、以下ではこの追加されたステップについてのみ説明する。

【０１５０】

順次集約のための一定期間が終了すると、証明装置7の監査情報作成部71は、監査装置8からの完全遅延補完データ要求に対して、この集約期間内に発行した各監査用受理証明書の完全遅延補完データを取得し、監査装置8に送信する（ステップS810、S820、S830、S840）。

【０１５１】

これにより、監査装置8は、各監査用受理証明書の完全遅延補完データを受信する（ステップS850）。

尚、図13に示すイベント順序証明方法においては、監査装置8の方から証明装置7に完全遅延補完データ要求を送信し、これに応えて証明装置7が監査装置8に完全遅延補完データを送信する方式であったが、これとは異なり、証明装置7が監査装置8に完全遅延補完データを自動的に送信するような方式であってもよい。

【０１５２】

次に、図14を参照しながら、監査装置3を用いたイベント順序証明検証方法について説明する。これは、利用者装置2iの第２の検証機能に相当するものである。ここで、利用者装置2iの第２の検証機能に関しては、第１の実施の形態の検証機能（「ユーザ点の未来側の境界付け」）に、新たな検証機能（「ユーザ点の過去側の境界付け」）が加わったものであり、この新たな機能の動作を示すのが図14である。即ち、本実施の形態の「ユーザ点の未来側の境界付け」に関する検証処理は、第１の実施の形態で示された図8の動作と全く同一であるため、説明は省略し、「ユーザ点の過去側の境界付け」に関する検証処理について説明する。また、利用者装置2iの第１の検証機能に相当する検証方法については、第１の実施の形態における検証方法と同一であるため、説明を省略する。

【０１５３】

まず、利用者装置2iは、監査の対象となる受理証明書（但し、即時補完データは含まれている）を含む監査要求情報を監査装置8に送信する（ステップＳ910、Ｓ920）。

【０１５４】

次に、監査装置8は送受信部31を介して監査要求情報を受信すると、イベント順序証明監査部82は、利用者装置2iから送信された監査要求情報に含まれる受理証明書が割り当てられた順次集約木のリーフτを特定し、該リーフτより左に位置する監査点α1を計算する（ステップS930，Ｓ940）。そして、この監査点α1の監査用受理証明書および該監査用受理証明書の完全遅延補完データを取得する（ステップS950）。

【０１５５】

続いて監査点α１のリーフτによる認証点を計算し、監査点α1の監査用受理証明書および該監査用受理証明書の完全遅延補完データから認証点の割当値A_{cal}を計算する（ステップS960、S970）。一方、イベント順序証明監査部82は、監査要求情報として既に受け取っている受理証明書の即時補完データからこの認証点の割当値Ａを取得して、この認証点の割当値Ａが、計算により求めた認証点の割当値A_{cal}に一致するか否かを検証する（ステップＳ980、Ｓ990）。

【０１５６】

以上の検証において、検証に成功すれば、受理証明書が改ざんされていないことを確認

することができる（ステップＳ995）。一方、検証に失敗すれば、受理証明書が改ざんされていることを確認することができる（ステップＳ1000）。そして、イベント順序証明監査部82は、この監査結果を送受部31を介して利用者装置2iに送信し、利用者装置2iは、監査結果を受信する（ステップS1010、Ｓ1020）。

【０１５７】

これにより、利用者装置2iは、電子的公表機関を介した公表前においても、証明装置7が発行した受理証明書が当該の順次集約期間において、受理証明書に含まれる元デジタル・データに対して、受理証明書に含まれる順次集約木リーフ番号で識別される順番において発行されたものであることを確実に検証することができるとともに、ユーザ点の過去側の境界付けを検証することができる。尚、上記監査結果に監査点α1の識別子を含めてもよい。この場合においては、利用者装置2iは、上記監査を要求した受理証明書に対応する証明要求の登録が、監査点α1に対応する監査用証明要求の登録より後であったことの保証を監査装置8から確実に得ることができる。

【０１５８】

尚、以上においては、「ユーザ点の過去側の境界付け」に関する検証処理の動作を説明したが、監査装置8は、「ユーザ点の未来側の境界付け」とともに「ユーザ点の過去側の境界付け」に関する検証処理を行うようにしてもよく、この場合には、監査要求情報として、第１の実施の形態における受理証明書および遅延補完データが必要となる。

【０１５９】

従って、第２の実施の形態のイベント順序証明システム200によれば、第１の実施の形態と同じ効果を得ることができる。また、これに加えて、受理証明書の正当性を検証できたときには、証明装置7において監査対象とした受理証明書の証明要求受信が監査に用いた監査用受理証明書の証明要求受信よりも時間的に後であることを証明することができる。

以上、第２の実施の形態について説明したが、第２の実施の形態には種々の変形例が考えられるものである。以下、第２の実施の形態の変形例について説明する。

【０１６０】

（２－３．第２の実施の形態の変形例1）

監査装置8は、上述した「ユーザ点の未来側の境界付け」及び「ユーザ点の過去側の境界付け」の機能から、２つのユーザ点の間の順序の判定を示すことも可能である。次に、２つの利用者装置2aと2bが各々、順次集約木リーフτとτ1において受理証明書を取得するとき、監査装置8がτとτ1の前後関係を監査する方法について図15を参照して説明する。ここで、図15は、監査装置8がτとτ1の前後関係を監査する動作を示すフローチャート図である。

【０１６１】

以下、順次集約木のリーフτ、τ1について、τ(或いはτ1)の時点とはτ(或いはτ1)に割り付けられた順序証明要求を受信した時点を表し、τ≦τ1と書くことにより、τの時点以降にτ1の時点があることを表す。以下では、τとτ1の大きい方をτ2とし、τ2で受信した順序証明要求に対する受理証明の送信の時点までは証明装置1の直列化可能性が保証されているものとする。

【０１６２】

尚、利用者装置2a及び2bと監査装置8は、それぞれ第１の実施の形態の「ユーザ点の未来側の境界付け」の説明で述べた条件（１）（２）及び（３）を満たすものとする。

【０１６３】

まず、監査装置8が、利用者装置2a及び2bより、各受理証明書のユーザ点間の順序判定要求を受けると、τに等しいか右に位置する監査装置8の監査点で最も左に位置するものをαとし、τ1に等しいか右に位置する監査装置8の監査点で最も左に位置するものをα1として、決定する（ステップS1110,S1120,S1130）。

【０１６４】

次に、監査点αとα１の時間的前後を比較する（ステップS1140）。これは、各監査点

の監査用受理証明書の順次集約木番号及び順次集約木リーフ番号から判断するものである。

【０１６５】

α＜α１のときは、第１の実施の形態の「ユーザ点の未来側の境界付け」及び上記「ユーザ点の過去側の境界付け」で述べた方法により、以下のようにτ＜τ１が示される（ステップS1150）。

【０１６６】

これは、τ１に等しいか左に位置する監査装置8の監査点でもっとも右に位置するものをα２とおくと、α≦α２であり、また、「ユーザ点の未来側の境界付け」で述べた方法により、τ≦αが示されるとともに、「ユーザ点の過去側の境界付け」で述べた方法により、α２≦τ１が示されるので、以上より、τ＜α≦α２＜τ１ となり、τ＜τ１ が導かれるものである。

【０１６７】

同様に、α１＜αのときは、τ１＜τが示される（ステップS1180）。

α＝α１のときは、τとτ１の前後関係の判定は、以下の手順（１）～（４）に従って行われる。

【０１６８】

（１）利用者装置2aがτとその遅延補完点τ'で取得する情報からユーザ点τの監査点αによる認証点の位置と割当値が計算され、監査装置8が監査点αで取得する監査用受理証明書に含まれる即時補完データに上記認証点の割当値が含まれていることにより、監査装置8はτが、αより左にあること、さらにτが、αより、幾つ左にあるかを判定する。ここで、τが、αよりn個左にあるものとする（ステップS1160）。

【０１６９】

（２）同様に、利用者装置2bがτ１とその遅延補完点τ１'で取得する情報からτ１の監査点αによる認証点の位置と割当値が計算され、監査装置8が監査点αで取得する監査用受理証明書に含まれる即時補完データに上記認証点の割当値が含まれていることにより、監査装置8はτ１が、αより左にあること、さらにτ１が、αより、幾つ左にあるかを判定する。ここで、τ１が、αよりn１個左にあるものとする（ステップS1160）。

【０１７０】

（３）ｎ＞ｎ１ のときは、監査装置8は、利用者装置2aによるユーザ点τが利用者装置2bによるユーザ点τ１より左に位置することを示すことができる（ステップS1170）。また、ｎ＜ｎ１のときは、監査装置8は、利用者装置2aによるユーザ点τが利用者装置2bによるユーザ点τ１より右に位置することを示すことができる（ステップS1170）。

【０１７１】

従って、第２の実施の形態の変形例１によれば、第２の実施の形態の効果に加えて、複数の受理証明書の時間的順序の判定をすることができる。

【０１７２】

（２－４．第２の実施の形態の変形例2）

また、監査装置8は、各順次集約期間の終了後に、その順次集約期間に取得した各監査用受理証明書の完全遅延補完データを取得する（複合完全補完を行う）と同時に、各監査用受理証明とその完全補完データから順次集約木のルート値を計算し、計算されたルート値が公表されたルート値に一致するか否かを検証することが可能である。このことを監査装置8による「複合完全化によるルート値検証」と呼ぶ。

【０１７３】

これは、図16に示すように、監査装置8が、順次集約木のルート値を計算し、計算したルート値が、証明装置7から公表されたルート値と一致するか否かを検証することで、証明装置7による不正が行われていないことを検証するものである（ステップS1210，S1220，S1230，S1240，S1250）。

【０１７４】

また、監査装置8は、この「複合完全化によるルート値検証」の機能により、利用者装

置2iからの監査要求に含まれる監査要求情報の正当性を検証することができる。

【０１７５】

例えば、ある順次集約木SBTの構成終了後に、利用者装置2aが、リーフ(0，τ)の割当値を本来の割当値V(τ)から割当値v'に改変し、割当値v'がV(root(SBT))にハッシュ関数hによりリンクすることを主張したとする。このとき、第三者にこの主張を認めさせるためには、利用者装置2aは、リーフ(0，τ）の補完データ

[(v(0)，LR(0))，(v(1)，LR(1))，…，(v(k-1)，LR(k-1))]

を用意し、v'とこの補完データをハッシュ関数hにより所定の方式で組み合わせることによりV(root(SVT))が計算できることを示さなければならない。この計算の過程においては、ユーザ点τの監査点αによる認証点（図９のp2）の割当値v2'も計算される。v2'はハッシュ関数の衝突困難性によって（実用上無視できる確率を除いて）round(α)において監査装置8に送付されたp2の割当値 V(p2)とは異なる。一方、監査装置8は、V(α)から出発し、authPath(α)に属するノードの割当値をハッシュ関数hによりリンクすることによりV(root(SBT))を計算する。p2 はauthPath(α)に属するので、V(p2)も結合される値の１つである。ここで（実用上無視できる確率を除いて）v2'≠V(p2)であるから、再びハッシュ関数の衝突困難性により、利用者装置2aが計算によって示す root(SBT)の割当値と監査装置8が複合完全化によるルート値検証において計算するroot(SBT)の割当値とは（実用上無視できる確率を除いて）異なることになる（この点についての詳細は、後述の順次集約木の性質4を参照）。従って監査装置8は利用者装置2aの主張が誤りであることを検出することができる。

【０１７６】

従って、第２の実施の形態の変形例２によれば、第２の実施の形態の効果に加えて、電子的情報公表機関が公表した順次集約木のルート値の正当性を検証することができる。また、監査装置8のルート値検証機能により、証明装置1及び利用者装置2iのいずれかにおいて不正があったとしても、不正の切り分けをすることができる。

【０１７７】

（２－５．第２の実施の形態の変形例3）

また、監査装置8は、利用者装置2iに完全補完データを提供する機能を備えることができる。以下、このことを補完データ完全化という。これは、証明装置7が障害などでサービス中断したときに有効に機能するものである。また、証明装置1がサービス中断しなくても、公表データ公開時や、補完データ要求が一時に大量に発生したときなどに証明装置7の負荷軽減に役立つものである。

【０１７８】

図17を参照して補完データ完全化について説明する。

【０１７９】

図17において、監査装置8が監査点aの完全補完データを持つならば、該完全補完データと利用者装置2iが、イベント受理証明書を取得するユーザ点uとその遅延補完データを取得する点u'で取得する情報を組み合わせることによりユーザ点uの完全補完データを計算することができる（以下、性質P1という）。

【０１８０】

なぜならば、図17で、j1はユーザ点uの監査点aによる認証点のレベルであり、ユーザ点uの認証パス情報のうち、レベルj1より小さいノードの情報はユーザ甲が取得しており、レベルj1以上k より小さいノードの情報は監査装置8が取得しているからである。但し、kは順次集約木の高さである。

【０１８１】

例えば、公開間隔が1週間とし、1日級の監査装置8(少なくとも１日に一回監査情報を取得し、各監査点の完全補完データを取得する機関）があるものとする。利用者装置2iは受理証明書を取得したのち、１日以上経過してから、遅延補完データを取得することにより、利用者装置2iの取得する情報と、監査装置8の取得する情報を組み合わせることにより利用者装置2iが取得した受理証明書の完全補完データを構成することができる（上記性質

P1による）。

【０１８２】

次に図18を参照して、２つ以上の監査装置8i（i=a，b，n）を介して利用者装置2iが完全補完データを取得する方法について説明する。尚、監査装置8iとしては、上述した１日級の監査装置8a（少なくとも１日に一回監査情報を取得し、各監査点の完全補完データを取得する機関）と監査装置8a依存の1時間級の監査装置8b（少なくとも1時間に一回監査情報を取得し、各監査点の遅延補完データ点を監査装置8aの監査点を挟むように設定する装置）があるとする。

【０１８３】

このとき利用者装置2iは受理証明書を所得したのち、１時間以上経過してから、遅延補完データを取得することにより、利用者装置2iの取得する情報、監査装置8bの取得する情報、及び監査装置8aの取得する情報を組み合わせることによりユーザ点の完全補完データを構成することができる。

【０１８４】

このことは、上記性質P1を繰り返し用いることにより示される。まず、監査装置8aの取得する情報と監査装置8bの取得する情報を組み合わせることにより、監査点a2の認証パス情報が得られる。従って、図17の場合の例と同様に、ユーザ点uの認証パス情報が得られる。

【０１８５】

尚、上述した監査装置8a及び8bの監査点に関する条件は、例えば、監査装置8a依存の1時間級の監査装置8bは、自己の各監査点の遅延補完データを１日以上たってから取得してもよいし、あるいは1日級の監査装置8aの監査点が1日の定時（例えば午前0時）に取得されることが分かっていれば、毎日の監査点の遅延補完データを、その日の終了後にまとめてとるようにしてもよい。また、上記例においては２つのレベルの監査装置8iを利用しているが、同様に３つ以上のレベルの監査装置8iを利用することも可能である。

【０１８６】

＜第３の実施の形態＞

（３－１．システム構成）

図19は、本発明の第３の実施の形態に係るイベント順序証明システム300のシステム構成図である。同図に示すイベント順序証明システム300は、イベント順序証明装置（以下、証明装置という）1、時刻情報提供装置30、複数の時刻証明利用者装置（以下、利用者装置という）10j（j=a，b，…，n）、複数のイベント順序証明利用者装置＆時刻証明装置（以下、利用者装置（時刻証明装置）という）20i（i=a，b，…，n）、イベント順序証明監査装置＆イベント時刻監査装置（以下、監査装置という）9、及び、以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成されるコンピュータネットワーク4を備えており、イベント順序証明を行うとともに、時刻証明を行うコンピュータシステムとなっている。即ち、利用者装置（時刻証明装置）20iは、上記実施の形態の利用者装置2iの機能に加えて、時刻証明を行う時刻証明装置の機能も備えており、利用者装置10jからの時刻証明要求に応えて、時刻受理証明書を発行し、利用者装置10jに返信するようになっている。また、利用者装置20iが、上記時刻受理証明書のダイジェストを含むイベント順序証明要求（以下、証明要求という）を証明装置1に送信すると、証明装置1は、該証明要求に応えて、イベント順序受理証明書（以下、受理証明書という）を発行し、利用者装置20iに返信するようになっている。そして、この受理証明書に疑義が生じた場合には、利用者装置20iは、証明装置1が公表したデータ又は監査装置9による監査結果によって受理証明書を検証することができるとともに、受理証明書と時刻受理証明書が対応付けられているので、区間時刻証を取得できるようになっている。

【０１８７】

尚、本実施の形態においては、上記実施の形態と異なる構成及び機能を説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

【０１８８】

また、上記実施の形態と同様に、第３の実施形態においても、イベント順序証明システム300のシステム構成は機能が同一であればその形態は問わないものであり、その物理的構成は種々考えられるものである。例えば、利用者装置（時刻証明装置）20iの代わりに、利用者検証装置（時刻証明装置）60iが受理証明書の検証を行うようにしてもよいし、証明装置1の代わりに、電子的情報公表装置5が証明装置1から公表データをもらい、公開するようにしてもよい。また、コンピュータネットワーク4は、郵便など他の通信手段に置き換えることも可能である。

【０１８９】

さらに、本実施の形態においても、第１の実施の形態と同様に証明装置１の直列化可能性は保証されているものとする。保証の手段としては、第１の実施の形態におけると同様、直列化可能性監査装置を用いることにしてもよい。

【０１９０】

時刻情報提供装置30は、正確な時刻情報を保持して、利用者装置（時刻証明装置）20i及び監査装置9に時刻情報を提供するようになっている。

【０１９１】

利用者装置10jは、利用者装置（時刻証明装置）20iに所定のデジタル・データを含む時刻証明要求をし、その応答として利用者装置（時刻証明装置）20iから時刻情報が付された時刻受理証明書を取得するようになっている。

【０１９２】

利用者装置（時刻証明装置）20iは、上述したように利用者装置2iの機能に時刻証明装置の機能を付加した装置で、コンピュータネットワーク4を介して証明装置1、監査装置9、利用者装置10j及び時刻情報提供装置30とデータを送受信する送受信部21、利用者装置10jからの時刻証明要求を受け付けて時刻受理証明書を作成する時刻証明作成部201、時刻受理証明書ダイジェストを含む証明要求を行うイベント順序証明要求部202、現時点において取得可能な受理証明書に対する補完データを要求する補完データ要求部23、受理証明書を検証するイベント順序証明検証部204、受理証明書をはじめとするイベント順序証明に関する情報及び時刻受理証明書をはじめとする時刻証明に関する情報を記憶する記憶部205を有する構成である。尚、本実施の形態においては、イベント順序証明利用者装置として、時刻証明装置を兼ねた利用者装置を採用しているが、時刻証明装置を兼ねない利用者装置が存在してもよく、利用者装置（時刻証明装置）20iと利用者装置2iが混在するようなシステム構成としてもよい。

【０１９３】

詳しくは、時刻証明作成部202は、利用者装置10jから送信された所定のデジタル・データを含む時刻証明要求を受け付けて、該デジタル・データに時刻情報提供装置30から取得した時刻情報を付した時刻受理証明書を作成するようになっている。

【０１９４】

イベント順序証明要求部203は、利用者装置10jからの時刻証明要求に対して作成された時刻受理証明書のハッシュ値である時刻受理証明書ダイジェスト（利用者装置（時刻証明装置）20iが予め用意した衝突困難一方向ハッシュ関数を時刻受理証明書に適用した結果）をイベント受理証明要求に含めるようになっている。従って、利用者装置（時刻証明装置）20iが、証明装置１から受信する受理証明書は、その構成において図4に示す通りであるが、元デジタル・データｙは、上述したように、時刻受理証明書ダイジェストを含むものとなっている。

【０１９５】

監査装置9は、第１の実施の形態の監査装置3の機能に加えて、時刻監査装置としての機能を備えており、詳しくは、コンピュータネットワーク4を介して証明装置1、利用者装置（時刻証明装置）20i及び時刻情報提供装置30とデータを送受信する送受信部31、利用者装置20iからある受理証明書の監査要求を受けた際には、利用者装置20iから送信された監査要求情報および監査情報を用いて受理証明書の検証を行い、その監査結果を利用者装置20iに返信するイベント順序証明監査部32、及び検証した受理証明書に対応する時刻受理

証明書に付された時刻の含まれる時間区間を証明する区間時刻証明証を作成する区間時刻証明証作成部91、監査用受理証明書、区間時刻証明証をはじめとする監査情報を記憶する記憶部92を有する構成である。尚、本実施の形態においては、イベント順序証明監査装置としては、イベント時刻監査装置を兼ねた監査装置を採用しているが、イベント時刻監査装置を兼ねない監査装置が存在してもよく、監査装置9と監査装置3が混在するようなシステム構成としてもよい。

【０１９６】

区間時刻証明証作成部91は、監査用受理証明書を証明装置1から受信したときの時刻を、時刻情報提供装置30から取得して、区間時刻証明証に付すようになっている。従って、区間時刻証明証作成部91で作成される区間時刻証明証には、本実施の形態においては、未来側の境界の時刻印が付されている。これは、第１の実施の形態で述べたように、監査装置3を用いたイベント順序証明検証（利用者装置2iの第２の検証）により、イベント受理証明要求が割り当てられた順次集約木のリーフが監査点のリーフよりも時間的に前であることが証明できるので、イベント順序証明要求の元となる利用者装置10iからの時刻証明要求の受付が、監査装置9が監査用受理証明書を受信した時刻よりも時間的に前であることを証明するものである。ここで、本実施の形態におけるこの区間時刻証明証を「第１種の区間時刻証明証」という。

【０１９７】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置（CPU：Central Processing Unit）、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置（メモリ）、ハードディスク（HD）等の電源断時にもデータを記憶し続けることが出来る２次記憶装置を有する電子的な装置から構成されている。このうち、利用者装置（時刻証明装置）20iの時刻証明作成部202、イベント順序証明要求部203、補完データ要求部204及びイベント順序証明検証部205、並びに監査装置9の区間時刻証明証作成部91の処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、利用者装置（時刻証明装置）20iの記憶部206及び監査装置9の記憶部92は、上記主記憶装置あるいは２次記憶装置の機能を備えたものである。

【０１９８】

また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置または２次記憶装置に格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ－ＲＯＭなどのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

【０１９９】

（３－２．システム動作）

次に、以上の構成を有するイベント順序証明システム300におけるイベント順序証明方法およびイベント順序証明検証方法を図20乃至23を用いて説明する。

【０２００】

尚、イベント順序証明方法においては、利用者装置（時刻証明装置）20iを利用者装置2i、監査装置9を監査装置3とすれは、全体的な動作は、図6に示す動作とほぼ同一であるため、異なる動作となる利用者装置（時刻証明装置）20iと利用者装置10j間のやりとりを中心に説明する。ここで、図20及び図21は、図６のステップＳ10に相当するイベント順序証明要求を送信するステップS10’を詳しく説明するシーケンス図である（図20においては、図６のステップＳ60に相当する受理証明書を受信するステップS60’も含む）。また、図22は、図６のステップＳ120に相当する監査用受理証明書を受信するステップS120’を詳しく説明するシーケンス図である。

【０２０１】

また、イベント順序証明検証方法の第１の検証においては、利用者装置20iを利用者装置2iとすれは、図７に示す動作と同一であるため、説明を省略する。また、イベント順序証明検証方法の第２の検証においては、監査装置9を監査装置3とすれは、図8に示す動作

とほぼ同一であるため、異なる動作となる監査装置9の区間時刻証の作成について説明する。ここで、図23は、図8のステップS520に相当するイベント受理証明書の検証に成功したときのステップS520' を詳しく説明するシーケンス図である。

【０２０２】

まず、図20を参照して、イベント順序証明方法のイベント順序証明要求を送信するステップS10'について説明する。

【０２０３】

利用者装置10j が利用者装置（時刻証明装置）20iにデジタル・データを含む時刻証明要求を送信すると、利用者装置（時刻証明装置）20iは送受信部201を介して、該デジタル・データを含む時刻証明要求を受信する(ステップＳ11'、Ｓ12')。次に、利用者装置（時刻証明装置）20の時刻証明作成部201は、時刻証明要求を受信した時刻を時刻情報提供装置30から取得し、デジタル・データに該時刻を付した時刻受理証明書を作成し、利用者装置10jに送信する(ステップＳ13'、Ｓ14、Ｓ15')。これにより、利用者装置10jは、時刻受理証明書を受信するので、時刻受理証明書を取得することができる(ステップＳ16')。

【０２０４】

次いで、利用者装置（時刻証明装置）20iのイベント順序証明要求部203は、時刻受理証明書のダイジェストを生成し、時刻受理証明書ダイジェストを含む証明要求を作成し、証明装置1に送信する（ステップＳ17'、Ｓ18）。この結果、証明装置1は、送受信部11を介して、証明要求を受信する（ステップS20'）。

【０２０５】

尚、上述した方法においては、利用者装置10jに時刻受理証明書だけを返信したが、図21に示すように、利用者装置10jに時刻受理証明書に加えて、受理証明書を返信する方法も考えられる。

【０２０６】

図21においては、ステップS10'のイベント順序証明要求ステップでは、時刻受理証明書を返信せずに、図６のステップＳ60に相当するステップS60'のイベント受理証明書受信ステップで、時刻受理証明書および受理証明書を返信する。即ち、利用者装置（時刻証明装置）20iは、証明装置1から受理証明書を受信すると、受理証明書および該受理証明書に対応する時刻受理証明書を利用者装置10jに送信するものである(ステップＳ61'，ステップＳ62')。これにより、利用者装置10jは、受理証明書および時刻受理証明書の双方を受信する（ステップＳ63'）。

【０２０７】

次に、図22を参照して、監査用受理証明書を受信するステップＳ120' について説明する。

【０２０８】

監査装置9は、送受信部31を介して証明装置1から監査用受理証明書を受信すると、監査用受理証明書を受信した時刻を時刻情報提供装置30から取得して、監査用受理証明書と対応付けて記憶部93に記憶する（ステップS121'、Ｓ122' 、Ｓ123'）。

【０２０９】

次に、図23を参照して、監査装置9によるイベント受理証明書の検証に成功したときのステップＳ520' について説明する。

【０２１０】

監査装置9のイベント順序証明監査部32が、利用者装置（時刻証明装置）20iからの監査要求に応えて受理証明書の監査を行い、監査結果がＯＫであるときには、さらに、監査用受理証明書に付された時刻から、第1種の区間時刻証明証を発行し、該区間時刻証明証を監査結果に含める（ステップS511'，S512' ，S513'）。

【０２１１】

従って、第３の実施の形態のイベント順序証明システム300によれば、第１の実施の形態と同じ効果を得ることができる。また、これに加えて、第1種の区間時刻証明証の発行

により、未来側の境界の時刻印を与えることができる。

【０２１２】

（３－３．第３の実施の形態の変形例）

第３の実施の形態においては、第１の実施の形態の監査装置3に時刻監査装置としての機能を備えた監査装置9を用いたが、第2の実施の形態の監査装置8に時刻監査装置としての機能を備えた監査装置9’を用いて第３の実施の形態の変形例としてもよい。

【０２１３】

この第３の実施の形態の変形例においては、区間時刻証明証作成部91’は、監査用証明要求を証明装置7に送信したときの時刻を、時刻情報提供装置30から取得して、区間時刻証明証に付すようになっている。従って、第３の実施の形態の変形例においては、区間時刻証明証作成部91’で作成される区間時刻証明証には、過去側の境界の時刻印が付されている。

【０２１４】

これは、第2の実施の形態で述べたように、監査装置8を用いたイベント順序証明検証（利用者装置2iの第２の検証）により、イベント順序証明要求が割り当てられた順次集約木のリーフがある監査点のリーフよりも時間的に後であることが証明できるので、イベント順序証明要求の元となる利用者装置10jからの時刻証明要求に対する利用者装置（時刻証明装置）20iによる時刻受理証明書の送信が、監査装置9’による監査用イベント順序証明要求の送信よりも時間的に後であることを証明するものである。ここで、この区間時刻証明証を「第2種の区間時刻証明証」という。

【０２１５】

また、第３の実施の形態の変形例においては、監査装置9’は、「第1種の区間時刻証明証」を発行する機能も当然に有するので、未来および過去側の境界の時刻印が付された区間時刻証明証である「第３の区間時刻証明証」を発行することが可能である。これは、イベント順序証明要求の元となる利用者装置10jからの時刻証明要求の受付が、監査装置9が監査用受理証明書を受信した時刻よりも時間的に前であることを証明するとともに、イベント順序証明要求の元となる利用者装置10iからの時刻証明要求に対する利用者装置（時刻証明装置）20iによる時刻受理証明書の送信が、監査装置9’による監査用イベント順序証明要求の送信よりも時間的に後であることを証明するものである。

【０２１６】

さらに、第３の実施の形態の変形例として、イベント順序証明システム300’は、利用者装置（時刻証明装置）20iの発行する時刻受理証明書と、該時刻受理証明書に付された時刻の時間的前、後、あるいは両方の境界を証明する１つ又は複数の区間時刻証明証を取得し、それに基づき時刻受理証明書に付された時刻の正当性を判定するイベント時刻検証装置（図19に図示せず）を有するシステム構成としてもよい。この場合においては、イベント時刻検証装置は、時刻受理証明書に付された時刻が、上記区間時刻証明証が証明する時間区間の中に、前もって定められた所定の誤差を許して含まれる割合が、前以て定められた所定の値より大きいことに基づき、時刻証明受理証明書に付された時刻の正当性を判定するようになっている。

【０２１７】

以上、本実施の形態について説明してきたが、本発明の要旨を逸脱しない範囲において、本発明の実施の形態に対して種々の変形や変更を施すことができる。例えば、上記実施の形態においては、順次集約木として二分木を用いたが、本発明は二分木に限定されるものではなく、１つの親が複数の子を持つ有向木であればよいものである。

【０２１８】

また、上記実施の形態において証明装置1及び7の電子的情報公表部17については特に詳しく述べなかったが、好適には、電子化社会における情報公表は以下のような要件を満たすことが求められる。

【０２１９】

(1) 複数の独立なエンティティが同一の情報を公表する。

【０２２０】
(2) 上記複数のエンティティの各々に誰でもがいつでもアクセスできる。
【０２２１】
(3) 上記複数のエンティティの各々が公表する情報を取得する際に、情報提供元のエンティティ認証が提供され、かつ提供される情報の完全性が保証される。
【０２２２】
上記の要件のうち、要件(1)については、複数のサービス機関が、ある範囲の情報について業務として提供することにより実現できる。上記実施の形態においては、証明装置と複数の監査装置が順次集約木のルート値等について業務として情報提供を行うことにより、この要件を満足するようにしている。
【０２２３】
要件(2)については、現在よく普及しているWWWにより情報提供することにより実現できる。
【０２２４】
要件(3)については、提供する情報に対して公開鍵暗号方式に基づくデジタル署名を付することにより実現できる。この際、デジタル署名の強度が十分強いこと、及びデジタル署名に用いた署名用秘密鍵及びとそれとペアになる公開鍵のその時点での有効性が、公開鍵証明書、CRL(Certificate Revocation List)、OCSPサービス(Online Certificate Status Protocol)等を用いて公開鍵基盤(PKI: Publike-Key Infrastructure)により保証されていることが必要となる。上記の鍵ペアのは、情報の要求者が情報を取得する時点で有効であれば十分であり、随時、鍵ペアを更新し、鍵ペアの有効性を保持しつづけることが可能となる。その際、あるキー・ペアKP1 ＝ (SK1, PK1) を新しいキー・ペアKP2 ＝ (SK2、 PK2)に置き換える際に、KP1が有効である間にKP2 の署名用秘密鍵 SK2 によるデジタル署名を生成することは必ずしも必要ではなく、利用者がアクセスした際に、その時点で有効なキー・ペアを用いてデジタル署名を生成することが要件となる。
【０２２５】
従来、情報公表手段として新聞等のマスメディアに情報を公表することが行われてきたが、この方法は例えば１０年後に特定のマスメディアに公表された情報にアクセスするのが容易ではないことから上記の要件(2)を満たすのが困難であること、さらにアクセスできたとしても上記の要件(3)を満たす形で情報を取得するのが困難であること等の理由で、電子化社会における情報公表の手段として必ずしも適当ではない。
【０２２６】
＜順次集約木の構成および性質＞
上記実施の各形態において用いられた順次集約木の動的な構成方法、および性質について説明するが、その前提としてまず、順次集約木の構成に必要な基本関数について説明する。
【０２２７】
（基本関数）
高さｋの順次集約木は、レベル0からレベルｋまでのノードで構成されるが、レベルｊ（ｊ＝0, 1, …, k）のノードの数は、$2^{(k-j)}$であるので、レベルｊ、番号ｉのノードを(ｊ, ｉ)と表すことにすると、ｉ＝0, 1, …, $2^{(k-j)}-1$となる。
【０２２８】
以下、実数xに対して、ceiling(x)をx以上の最小の整数、floor(x)をx以下の最大の整数として、説明する。
【０２２９】
ノード（ｊ, ｉ）（但し、ｊ＜ｋ）の親は、（ｊ＋1, floor(i/2)）であるので、
parent(j, i)＝（ｊ＋1, floor(i/2)）
と定義する。また、ノード（ｊ, ｉ）（但し, 0＜j）の左側の子供は（j−1, 2・i）、右側の子供は（j−1, 2・i＋1）であるので、
leftChild(j, i) ＝（j−1, 2・i）

rightChild(j, i) ＝ (j－1, 2・i＋1)

と定義する。このとき、高さkの順次集約木のノード(j, i) ($0 \leqq i < 2^{(k-j)}$) のルート・パス$rtPath_k(j, i)$ (ノード(j,i)からルートに至るノードの列をいう)は、

$rtPath_k(j,i)$＝[(j,r(j)), …, (k,r(k))]

と表すことができる。但し、r(j)＝i, r(j'＋1)＝floor(r(j')/2) (j'＜kとし、r(j')は既に定まっているものとする) であるとする。尚、(k, r(k)) は、順次集約木のルートを表し、常にr(k)＝0となる。

【０２３０】

V(j, i) はノード(j, i) の割当値である。V(0, i) をV(i)と書く。LをL≦k なる非負整数、SBTをある順次集約木とするとき、SBTの部分グラフBがレベルLの部分木であるとは、SBTに属するレベルL のあるノードpがあり、B がp 及び p の子孫からなるSBT の部分グラフとなっていることと定義する。

【０２３１】

B がSBTの部分木であるとき、leafs(B)はBのリーフの集合を表すものとする。またX をSBTのリーフからなる空でない集合とするとき, first(X) によりX のうち最も左に位置するリーフを表し、last(X)によりXのうち最も右に位置するリーフを表す。

【０２３２】

２つの整数i1, i2 について, [i1..i2] はi1 ≦i ≦i2 なる整数iからなる集合（区間）を表し、(i1..i2] はi1 ＜i ≦i2 なる整数iからなる集合（区間）を表し, [i1..i2) はi1 ≦i ＜i2 なる整数iからなる集合（区間）を表し、(i1..i2) はi1 ＜i ＜i2 なる整数iからなる集合（区間）を表すものとする。

【０２３３】

（順次集約木の構成方法）

・第1の順次集約木の構成方法

上述した基本関数の定義のもと、第１の動的な集約木の構成方法について説明する。この集約木の構成方法は、深さの違いを1以内に押さえ、ダミー・ノードを作成しない方法である。

【０２３４】

集約期間（例えば１週間）に受付けるるイベント順序証明要求の数が何らかの方法により前以てさだまっているものとし、その数をｎとする。このとき、集約木の高さｋは，ｋ＝ceiling($\log_2$(N))である。高さｋの順次集約木リーフ数は最大で2^kであるので、ｄ＝2^k－ｎとして、レベル0のノードのうち，2ｄ個を消去すれば、イベント順序証明要求の数ｎをダミー・ノードなしでリーフに割り当てることが可能となる。これは、レベル0のリーフが2ｄ個減ると、レベル1のリーフが新たにｄ個できるので、合計でｄ個減り、リーフの数は結局、2^k－ｄ＝ｎとなるからである。

【０２３５】

以下、LIW＝$2^{(k-1)}$（レベル1のノードの個数）、LIL＝$2^{(k-1)}$－ｄ（子を有するレベル1のノードの個数）の、LOL＝2($2^{(k-1)}$－ｄ)（レベル0のノードの個数）とおくと、ｎ個のイベント順序証明要求のうち、初めのLOL個をレベル0に配置し、残りをレベル1に配置するとき、ｉ番目のイベント順序証明要求の配置先を表す関数place(i)は次式で表すことができる。

【０２３６】

place(i)＝ (0, i)　　(0≦i＜LOL)

place(i)＝ (1, LIL ＋ i －LOL)　　(LOL ＜ i ≦ n)

ここで、place(i)＝（レベル，番号）で構成されているものである。

【０２３７】

図24は、第１の動的な集約木の構成方法のｎ＝10の場合の具体例を示すものである。この場合においては、図24に示す通り、ｋ＝ceiling($\log_2$(10))＝4となり、高さは4である。そして，ｄ＝2^4－10＝6であるので、6×2＝12個のレベル0のリーフを消去する。この結果、LIW＝2^3＝8，LIL＝8－6＝2，LOL＝2×2＝4となる。従って、レベル0のリーフが4個、

レベル1のリーフが6個で，リーフの合計数はｎ＝10となる。この結果、図24に示すような集約木を動的に作成することができる。レベルが0より大きいノード（即ちリーフではないノード）に対する値の割当は、それが可能になったときにインクリメンタルに行われる。

【０２３８】

・第２の順次集約木の構成方法

次に、第２の動的な順次集約木の構成方法について説明する。この方法はインクリメンタルに集約木を構成する点では第１の方法と同じであるが、前もって定めた時間間隔（順次集約期間）に受付けるイベント順序証明要求の数は予想できないものと仮定している点が第１の方法と異なる。

【０２３９】

ここで、インクリメンタルとは、イベント順序証明要求を受付ける都度、そこから計算できる順次集約木の部分を計算していくという意味である。以下では、受付けるイベント順序証明要求の数は予想できないが、その上界Ｎは見積もることができるとして説明する。この方法においては、イベント順序証明要求はすべてレベル0に割り付けられるものとし、二分木のルート値を計算するためにダミー・ノードを使用する方法である。

【０２４０】

この方法で順次集約木を構成するとき、所定の集約期間（例えば、１週間）に受付けたイベント順序証明要求の数をNとすると、順次集約木をの高さｋは、$k = ceiling(\log_2(N))$である。高さｋの順次集約木リーフ数は最大で2^kであるので、0からｎ－1までのｎ個のイベント順序証明要求をレベル0のノード（0，0）からノード（0，ｎ－1）に割り当てられることになる。

【０２４１】

レベル0に割り当てられた、最も右のノード（0，ｎ－1）に対して、ルート・パス $rtPath_k(0, n-1)$が

$$rtPath_k(j, i) = [(j, r(j)), \cdots, (k, r(k))]$$

と表現されるものとする。

【０２４２】

（一般に、$rtPath_k(j, i)$は、$rtPath_k(j, i) = [(j, r(j)), \cdots, (k, r(k))]$

と表現される。但し、$jl \in [j..k]$に対して$r(jl) = floor(i/2^{(jl-j)})$とする。）

このとき、各レベルｊ（ｊ＝0，…，ｋ－1）においては、以下のことが成り立つ。

【０２４３】

r(j)が偶数のとき、ノード（j，r(j)＋1）はダミー・ノードとなり、

$r(j)+1 < i < 2^{(k-j)}$となる各ｉに対して、ノード（ｊ，ｉ）は消去されている。

【０２４４】

r(j)が奇数のとき、$r(j)+1 < i < 2^{(k-j)}$となる各ｉに対して、ノード（ｊ，ｉ）は消去されている。

【０２４５】

以上のような方法に基づいて構成される順次集約木は、ダミー・ノードは各レベルの右端でのみ現れる、および作成されるダミー・ノードの数は、ｋ以下であるという性質を有する。

【０２４６】

図25及び 図26は、第２の順次集約木の構成方法のアルゴリズムを示すものであり、該アルゴリズムに従って順次集約木がインクリメンタルに構成されるようになっている。ここで、前提として以下の定義を行う。

【０２４７】

・$K = ceiling(\log_2(N))$とする。

【０２４８】

・nは受付けたイベント順序証明要求の数を示す整数変数とする。初期値は0である。

【０２４９】

・kは定められた時間間隔が終了したときの順次集約木の高さを表す変数とする。

【０２５０】

（K＋1）個のカウンタの列を，i_0，…，i_Kとする。ここで、i_jの初期値は0である（j＝0，…，K）。i_jはレベルjにおいて、既に生成されたノードの数を表すと同時に、次にレベルjに作成されるノードの番号を表す。

【０２５１】

・（K＋1）個のブール変数の列を、b_0，…，b_Kとする。ここで、b_jの初期値はfalseである（j＝0，…，K）。b_jは、レベルjにダミー・ノードがあるか否かを表す。

【０２５２】

・（K＋1）個の配列の列を、A_0，…，A_Kとする。各配列は、$2^{(K-j)}$の長さをもち、レベルjのノードに割り付けられる値を保持する（j＝0，…，K）。

【０２５３】

・rはダミー・ノードに割り当てるダミー値を保存する変数である。

【０２５４】

・R(j，i)は2つの引数i，jに対してノード(j，i)に割り当てるべきダミー値を計算する関数である。

【０２５５】

・x，x0，x1，x2は、ノードに割り当てる値を表す変数である。

【０２５６】

・x1‖x2は、ビット列で表された2つの値の連接である。

【０２５７】

・h(x) はxのハッシュ値を計算する衝突困難一方向ハッシュ関数である。

【０２５８】

このような定義のもと、図25の処理手順1が終了すると（即ち所定の順次集約期間が終了すると）、nは受付けた時刻処理要求の数，kは生成された順次集約木の高さ，i_jはレベルjのノードの数，b_jはレベルjにダミー・ノードがあるか否か、A_jは，レベルjのノードに割り付けられた値からなる配列をそれぞれ表すことになる。

【０２５９】

図27は、第２の動的な順次集約木の構成方法のｎ＝9の場合の具体例を示す図である。即ち、定められた順次集約期間が終了したとき、ｎ＝9であったとする。このとき、ｋ＝ceiling($\log_2(9)$)＝4となり、高さは4の順次集約木を構成することになる。尚、0からｎ－1までのｎ個の順序証明要求は、処理手順1により、既にノード(0，0)，…，(0，n－1)に割り当てられている。また、処理手順1により、i_0＝9，i_1＝4，i_2＝2，i_3＝1，i_4＝0となっている。

【０２６０】

このとき、処理手順2の(2.2)から、ノード(0，8)のノードパス$rtPath_4(0,8)$は

$rtPath_4(0,8)$＝[(0，8)，(1，4)，(2，2)，(3，1)，(4，0)]

となる。これから、各レベルの手順は、以下の通りになる。

【０２６１】

レベル0においては、ステップ（2.3.2.1）より、ノード（0，9）がダミー・ノードになる。レベル1においては、ステップ（2.3.3.1.5）より、ノード（1，4）に値が割り付けられ、(1，5)がダミー・ノードになる。レベル2においては、ステップ（2.3.3.1.5）より、ノード（0，2）に値が割り付けられ、(0，3)がダミー・ノードになる。レベル3においては、ステップ（2.3.3.1）により、ノード（3，1）に値が割り付けられる。レベル4においては、ステップ（2.3.3.1）により、ノード（4，0）に値が割り付けられる。

【０２６２】

この結果、図27に示すような順次集約木をインクリメンタルに構成することができる。ダミー・ノードは各レベルに於いて高々１つである。ダミー・ノードには前以て定められた何らの手順に従いダミー・ラベル（ダミー割当値）を割当てる必要があるが、このような手順の簡単な定義としては、レベルの関数としてダミー・ラベルを定義する方法があり

、これを採用してもよい。
図28は、上記のインクリメンタルな順次集約木の構成方法において各ノードに値を割付けるタイミングを示したものである。
【０２６３】
上述の第1及至第３の実施の形態においては、順次集約木は 図28に示すように、情報公表の区切りにおいては、ダミー・ノードを用いて最終的な順次集約木の構成する方式を前提としている。しかし、順次集約木の具体的な構成法としてこれ以外の方法を採用することも可能である。
【０２６４】
即ち、上記実施の形態におけるイベント順序証明システム100、200及び300は、上述した動的な集約木の構成方法のいずれをも採用できるものであり、これにより、利用者装置からのイベント順序証明要求の量的変化に柔軟に対応することができるので、スケーラビリティの高いイベント順序証明システムを構築することが可能となる。
【０２６５】
（認証パスの定義とそれによるルート値の計算法）
予め高さが決定しておらずインクリメンタルに構成されるような順次集約木のノードに対して、ある時点のルート・パスや認証パスを以下のように定義することができる。この定義は第1及至第３の実施の形態において所定の順次集約期間に受付ける要求の数が前以て予想できないときに適用することができる。
【０２６６】
現時点のリーフ番号の最大値がm(≧0) (従ってリーフの数が m＋1)のとき、
$\kappa(m) = \min\{h \mid m+1 \leqq 2^h\}$ とおく。
高さが $\kappa(m)$ の順次集約木を
curSBT(m)
とおく。
【０２６７】
p＝(j, i) ∈curSBT(m) とし、pから curSBT(m)のルートに至るノードの並びルート・パスと言いを
rtPath(p, m)
と書く。
【０２６８】
rtPathD(p, m)は、rtPath(p, m)に属するノードのうちでm番目のリーフの割当値が定まった時点で割当値が定まっている ノード の列である。
【０２６９】
rtPath(p, m) ＝ [(0, i(0)), …, (k, i(k))]
としたとき、 0 ≦ k1 ≦ k なるあるk1 があって、
rtPathD(p, m) ＝ [(0, i(0)), …, (k1, i(k1))]
となることが分かる。
【０２７０】
rtPathDV(p, m) は、 rtPathD(p, m) の各ノードに割当値を割り当てたものである。
【０２７１】
rtPathD(p, m) ＝ [(0, i(0)), …, (k1, i(k1))]
のとき、rtPathDV(p, m) は次のような形となる。
【０２７２】
rtPathDV(p, m) ＝ [((0, i(0)), v(0)), …, ((k1, i(k1)), v(k1))]。
【０２７３】
curSBT(m) における、ノード p ＝(j, i) からcurSBT(m)のルート値を計算するのに必要なノードp'＝(j', i')の集合を該ノードの認証パスと呼びauthPathT(p, m)と表す。但し、認証パスに属する各ノードについて、該ノードを連接する方向（左又は右）についての情報もタグとして含んでいるものとする。

【０２７４】
$\kappa(m) = k$ で、
rtPath(p, m) = [(j, r(j)), …, (k, r(k))]
のとき，authPathT(p, m)はrtPath(p, m) を用いて次のように表すことができる。
【０２７５】
authPathT(p, m)＝
[((j, a(j)), LR(j)), …, ((k－1, a(k－1)), LR(k－1))]
ここで、r(j')が偶数の場合，a(j')＝r(j')＋1、r(j')が奇数の場合、a(j') ＝r(j')－1であり、また、r(j')が偶数の場合、LR(j')＝R，r(j')が奇数の場合，LR(j')＝Lである（但し、$j' \in [j..k-1]$）。
【０２７６】
そして、authPathT(p, m)の要素 ((j, a(j)), LR(j))について、LR(j)の部分を（LR）タグという。さらに、rtPath(p, m)の要素 (j, r(j))について、r(j)が偶数のとき、（j, r(j)＋1）を(j, r(j))の右補完点といい、r(j)が奇数のとき、(j, r(j)－1)を(j, r(j))の左補完点という。
【０２７７】
このとき、authPathT(p, m)は、rtPath(p, m)のルート以外の点の右補完点あるいは左補完点からなる。
【０２７８】
またauthPathT(p, m) からLRタグの情報を除いたものを authPath(p, m) と書く。即ち、
authPathT(p, m)＝
[((j, a(j)), LR(j)), …, ((k－1, a(k－1)), LR(k－1))]
であるとき、
authPath(p, m)＝[(j, a(j)), …, (k－1, a(k－1))]
とする。逆に
authPath(p, m)＝ [(j, a(j)), …, (k－1, a(k－1))]
が与えられればauthPathT(p, m)を以下のように計算できる。 $jl \in [j..k)$に対して、rtPath(p, m) のレベルjlのノードは
$(jl, floor(i/2^{(jl-j)}))$
となるので、 $floor(i/2^{(jl-j)})$ が偶数であるときLR(jl) ＝ R，奇数であるとき LR(jl) ＝ L と定め、
authPathT(p, m)＝
[((j, a(j)), LR(j)), …, ((k－1, a(k－1)), LR(k－1))]
とおけばよい。従って、authPathT(p, m) とauthPath(p, m) の一方から他方を計算することが出来る。
【０２７９】
authPath(p, m) 及び authPathT(p, m)の中で，m番目のリーフの割当値が定まった時点で割当値が定まっているノードの集まりを各々
authPathD(p, m) 及び authPathTD(p, m)
と定義する。authPath(p, m) 及び authPathT(p, m)が上記のように表現されるとき、
$kl \leq k - j$ なる kl と、
$j \leqq j(0) < j(1) < \cdots < j(kl - 1)$
なる非負整数 j(0), …, j(kl － 1)があり、
authPathD(p, m)＝[(j(0), a(j(0))), …,
(j(kl－1), a(j(kl－1)))],
authPathTD(p, m)＝[((j(0), a(j(0))), LR(j(0))), …,
((j(kl－1), a(j(kl－1))), LR(j(kl－1)))],
と表現される。
【０２８０】

さらに、authPathD(p, m) 及びauthPathTD(t, m)に、それに属するノードの割当値を加えたものを、各々authPathDV(p, m) 及びauthPathTDV(p, m)と置く。具体的には、authPathD(p, m)及びauthPathTD(p, m)が上記のように表現されるとき、

authPathDV(p, m)＝
[((j(0), a(j(0))), v(j(0))), …,
((j(kl－1), a(j(kl－1))), v(j(kl－1)))],
authPathTDV(p, m)＝
[((j(0), a(j(0))), LR(j(0)), v(j(0))), …,
((j(kl－1), a(j(kl－1))), LR(j(kl－1)), v(j(kl－1)))]

とおく。ここで、各j'∈{j(0), …, j(kl-1)} に対して、v(j') ＝ V(j', a(j')) である。

【０２８１】

上述の順次集約木の構成法の何れかの方法により、リーフ番号mのリーフに順次割当値を割り当てた段階で当該の順次集約木の構成が終了し、かつauthPathTDV(p, m)が上記のように表されるとき、ノードp ＝ (j, i) の割当値V(p) とauthPathTDV(p, m)から以下のようにして集約木のルート値を計算することができる。jl ∈[j..k] に対して、v'(jl)を以下(1), (2) により再帰的に定義する。このとき、v'(k) が集約木のルート値となる。

【０２８２】

(1) v'(j) ＝ V(j, i)
(2) jl ∈[j..k]に対して，v'(jl) が定義されたとする、LR(jl) ＝ L のとき、
v'(jl+1) ＝ h(v(jl)‖v'(jl))
LR(jl) = R のとき、
v'(jl+1) ＝ h(v'(jl)‖v(jl))
と定義する。

【０２８３】

ml, m2 を順次集約木リーフ番号とし、ml ≦ m2 とする。このとき、
curSBT(ml) ⊆ curSBT(m2) である。

【０２８４】

p ＝ (j, i) ∈curSBT(ml)とする。このとき、以下の(1), (2), (3) が成立つ。

【０２８５】

(1) rtPath(p, ml) ⊆ rtPath(p, m2)
(2) authPath(p, ml) ⊆ authPath(p, m2)
(3) authPathD(p, ml) ⊆ authPathD(p, m2)

＜順次集約木の諸性質＞

以下では、インクリメンタルに構成される順次集約木について、現時点のリーフ番号の最大値をm とし、

rtPath((0, i), m), rtPathD((0, i), m), rtPathDV((0, i), m)

を各々短く

rtPath(i, m), rtPathD(i, m), rtPathDV(i, m)

と書くこともある。同様に

authPath((0, i), m), authPathT((0, i), m), authPathD((0, i), m),
authPathTD((0, i), m), authPathDV((0, i), m), authPathTDV((0, i), m)

を各々短く

authPath(i, m), authPathT(i, m), authPathD(i, m),
authPathTD(i, m), authPathDV(i, m), authPathTDV(i, m)

と書くこともある。

【０２８６】

次に、順次集約木において、ユーザ点の監査点による認証点を計算するアルゴリズムについて説明する。前提として、順次集約木の高さをｋとし、ユーザ点の識別番号をi0、監

査点の識別番号をi1とし、i0<i1とする。一般に、順次集約木のノード(0, i)に対してrtPath((0, i), m) は以下のように計算できる。

【０２８７】

rtPath((0, i), m) ＝ [(0, r(0)), …, (k, r(k))]

但し、k＝κ(m), j∈[0..k]に対して r(j) = floor(i/2^j)と置く。

【０２８８】

この手順によって、ノード（0, i0）のルート・パス rtPath((0, i0), m)とノード（0, i1）のルート・パス rtPath((0, i1), m) を計算する。すると、rtPath((0, i0), m)とrtPath((0, i1), m)は、ある要素以降は一致する。このとき、最初に一致した要素を、ノード（0, i0）とノード（0, i0）の合流点（confluent point）と呼ぶ。そして，合流点のレフト・チャイルドを、ノード（0, i0）（ユーザ点）のノード（0, i1）（監査点）による認証点（authentication point）とよぶ。

【０２８９】

以上は、ユーザ点と監査点が同一の順次集約木に属する場合における認証点の定義であるが、該ユーザ点が属する順次集約木SBTより後に、該監査点の属す順次集約木の属する順次集約木が生成される場合には，SBTのルートを該ユーザ点の該監査点による認証点と定義する。

【０２９０】

（順次集約木の性質１）

B を ある順次集約木の部分順次集約木で、ある時点において、last(leafs(B)) に対応するラウンドの処理が終了済みとする。このとき、その時点においてB に属する各ノードの割当値は計算され割当てられている。

【０２９１】

・性質１の証明

図25及び図26で示されるインクリメンタルな順次集約木の構成法により、各ラウンドの終了時には、そのラウンドまでに取得できたリーフの割当値により計算できるリーフ以外のノードの割付値は全て計算され該ノードに割当てられることになる。

【０２９２】

last(leafs(B))に対応するラウンドの処理が終了したときには、leafs(B)に属する各リーフの割当値は定まっており、従ってBの各ノードの割当値が計算できる。従って、この段階で、Bの各ノードの割当値は計算され、各ノードに割当てられている。

予め高さが決定しておらずインクリメンタルに構成されるような順次集約木に対して、次の性質2がなりたつ。

【０２９３】

（順次集約木の性質2）

C を利用者装置、乙 を監査装置とし、i0 と i1 を i0 ＜ i1 なる二つの順次集約木リーフ番号とし、round(i0) において、C は受理証明書を受信し、乙 はround(i1) において監査用受理証明書を受信したものとする。このとき、i0 の i1 による認証点は以下の性質を持つ。

【０２９４】

（1）認証点の割当値は、監査点、即ちノード（0, i1）の受理証明書内補完データに含まれる。

【０２９５】

（2）上記認証点を(j', i') とおくと、authPath((0, i0), i1)に属するノードで、レベルがj'より小さいものに対する割当値は、ノード（0, i1）に対応するラウンドで受理証明書を受理した利用者が、ノード（0, i1）に対応するラウンド以降において受信できる遅延補完データあるいは受信した受理証明書内補完データに含まれる。

【０２９６】

即ち、i1 ≦ i2 とすると，authPath((0, i0), i1)に属するノードで、レベルがj'より小さいものに対する割当値は，EOC(i0) あるいはCToken(i0, i2) に含まれる。

【０２９７】
(3) 上記認証点の割当値及びrtPath((0, i0), i2)に属するノードでレベルが該認証点のレベルより小さいノードの割当値は、ノード（0, i0）で受理証明書を受理した利用者が、ノード（0, i1）に対応するラウンド以降において受信する遅延補完データおよびノード(0, i0)で受信した受理証明書（受理証明書内補完データを含む）から計算することができる。

【０２９８】
・性質2の証明

以下では、利用者に渡す受理証明書に、受理証明書内補完データ（即時補完データ）を含める場合について説明する。利用者に渡す受理証明書に受理証明書内補完データを含めず、その代わりに遅延補完データにこの情報を含める場合でも同様の議論により同じ結論が得られる。

【０２９９】
(1) まず、項目（1）について図29を用いつつ説明する。ここで、合流点を（j, i）、そのレフト・チャイルドである認証点を（j', i'）とおく。ノード（0, i1）のcurSBT(i1)におけるルート・パス rtPath((0, i1), i1)において、（0, i1）から出発して、合流点に至る直前のノードを（j", i"）とおく。このとき、認証点は，（j", i"）の左補完点である。従って、認証パス authPathT(i1, i1)の定義から、((j', i'), L)はノード（0, i1）のcurSBT(i1) における認証パスに含まれる。また，ノード(j', i')への値の割当ては，round(i1)より前に終了している。 よって、((j', i'), L, V(j', i'))は（0, i1）に対する受理証明書内補完データに含まれる。

【０３００】
(2) 次に項目（2）について図30および図31を用いつつ説明する。

【０３０１】
k = κ(i1) とおく。

【０３０２】
認証点（j', i'）はノード（0, i0）のルート・パス rtPath((0, i0), i1) に含まれる。ここで、

rtPath((0, i0), i1) ＝
[(0, r(0)), …, (j', r(j')), (j'＋1, r(j'＋1)), …, (k, r(k))]

とする。

【０３０３】
また、authPath((0, i0), i1) の要素で、レベルがj'より小さいノードの並びを
[(0, s(0)), …, (j'－1, s(j'－1))]
とおく。

【０３０４】
各j1 ∈ [0..j'－1] に対して，V(j1, r(j1))がEOC(i0)あるいはCToken(i0, i2)に含まれることを示せばよい。

【０３０５】
authPath((0, i0), i1)の定義により、
authPath((0, i0), i1)のレベル j1の要素 p2＝(j1, s(j1))は，rtPath((0, i0), i1)のレベルj1＋1の要素 p3＝(j1+1, r(j1+1))のライト・チャイルドであるか或いはレフト・チャイルドである。どちらであるかによって場合分けする。

【０３０６】
（場合1）p2がp3のライト・チャイルドであるとき、図30に示すように、p2の割当値V(p2)は、i1≦i2なi2において，Cが受信できる遅延補完データ CToken(i0, i2) に含まれる。なぜならば、順次集約木の性質1により、リーフ(0, i1) に対応するラウンドのイベント順序証明処理が終わった時点で、図30のBで表された curSBT(i1) の部分木の割当値は計算可能であり計算され割当て済みである。従って、その時点以降で発行される遅延補完データにはBのルートp2の割当値V(p2)が含まれる。

【０３０７】
（場合2）p2がp3のレフト・チャイルドであるとき、図31に示すように、ノードp2の割当値V(p2)は、round(i0)のイベント順序証明要求者に対するト受理証明書内補完データに含まれる。何故ならば、図31 の p2をルートとする部分木B について、

$$\forall i \in leafs(B)[\, i < i0 \,]$$

であり、従ってB ⊆ curSBT(i0)でかつ i0で識別されるラウンドの開始時に、leafs(B)の割当値は確定している。よって 順次集約木の性質１により、p2 ＝ root(B)の割当値は、i0で識別されるラウンドにおいて確定している。従って、p2 はauthPathD((0, i0), i0)に含まれる。

【０３０８】
(3) 認証パスの定義及び項目(2)から、各j1∈[0..j']に対して、V(j1, r(j1)) を以下のように再帰的に計算することが出来る。

【０３０９】
まず、V(0, r(0)) はイベント受理証明書に含まれているノード(0, i0) の割当値とする。

【０３１０】
次に、j1∈[0..j'－1)に対して，V(j1, r(j1)) が計算されたと仮定し、V(j1+1, r(j1+1))を以下のように計算する。r(j1) ＜ s(j1) のときは、

$$V(j1+1,\ r(j1+1)) = h(V(j1,\ r(j1)) \| V(j1,\ s(j1)))$$

とし，s(j1) ＜ r(j1) のときは、

$$V(j1+1,\ r(j1+1)) = h(V(j1,\ s(j1)) \| V(j1,\ r(j1)))$$

とする。

【０３１１】
以下では、時刻の原点として、イベント順序証明システムのサービス開始時点をとり、時間を計る単位として１秒、１ミリ秒等を定め，時刻を，上記の原点から上記の時間の単位で計った整数で表現するものとする。また，各監査装置 乙 は、各順次集約期間 Tの最初の監査点においては、T に閉じた監査情報に加えて、前順次集約ルート値（直前の順次集約期間 T' の ルート の割当値 V(root(T'))） も受信するものとする。

【０３１２】
予め高さが決定しておらずインクリメンタルに構成されるような順次集約木に対して次の性質3がなりたつ。

【０３１３】
（順次集約木の性質3）
以下では、T を正整数とし，α，α0，τ，τ' は拡張リーフ識別子を表すものとする。乙は監査装置とし、乙の監査点α0で、次の条件(*1) 満たすものが存在するものとする。

【０３１４】
(*1) time(α0) ∈[0..T)
さらに乙による任意の１つの監査点をα，その次の乙による監査点をα' とすると次の条件(*2)が成り立つものとする。

【０３１５】
(*2) time(α') － time(α) ≦ T
また、利用者 甲 はあるイベント順序証明要求を送信し、その要求に対応する順次集約木リーフをτ，その後、該イベント受理証明書に対する遅延補完データ要求し、その要求に対応する順次集約木リーフをτ' とすると次の条件(*3) が成り立つものとする。

【０３１６】
(*3) time(τ') － time(τ) ≧ T
さらに、監査装置乙は２番目以降の各順次集約期間に属する乙による最初の監査点において、直前の順次集約期間のルート値をイベント順序証明機関から受信するものとする。

【０３１７】

このとき，以下の(1)及至(4)　が成り立つ。

【０３１８】

(1) $\alpha \in [\tau..\tau']$ となる乙によるある監査点αが存在する。

(2) $\alpha \in [\tau..\tau']$ となる乙による監査点αについて、τ の α による認証点の割当値（ラベル）は、α 以後のある順次集約木リーフ（例えばτ'）において 乙 が受信する監査用受理証明書に含まれる。

【０３１９】

(3) 任意の順次集約木リーフτに対して、乙による監査点α'があり、次の条件(*4)が成立つ。

【０３２０】

(*4) $time(\tau) \leqq time(\alpha') < time(\tau) + T$

(4) $T \leqq time(\tau)$となる任意のユーザ点τについて，$\alpha < \tau$となる乙の監査点αが存在する。

【０３２１】

・性質3の証明

(1) $\alpha \in [\tau..\tau']$ となるような乙によるある監査点αが存在しないと仮定する。τより左に位置する乙による監査点が存在するか否かにより場合分けする。

【０３２２】

（場合１）τより左に位置する乙による監査点が存在する場合を考える。 τ より左に位置し、τに最も近い乙による監査点を$\alpha 1$とし、τ' より右に位置しかつ τ' に最も近い乙による監査点を $\alpha 2$ とする。$\alpha 1$ と $\alpha 2$ のとり方より、

$time(\alpha 1) < time(\tau)$ 及び$time(\tau') < time(\alpha 2)$

が成り立つ。 $time(\alpha 1) < time(\tau)$ より，$-time(\alpha 1) > -time(\tau)$ となる。

【０３２３】

従って、

$time(\alpha 2) - time(\alpha 1) > time(\tau') - time(\tau) \geqq T.$

一方，$time(\alpha) \in [time(\tau)..time(\tau)]$ となるような乙によるある監査点αが存在しないのであるから、$\alpha 2$ は $\alpha 1$ の次の監査点である。従って上記条件(*2)より、

$time(\alpha 2) - time(\alpha 1) \leqq T$ とならなければならない。以上から、

$time(\alpha 2) - time(\alpha 1) > T$ かつ $time(\alpha 2) - time(\alpha 1) \leqq T$

となり矛盾が導かれる。従って、$time(\alpha) \in [time(\tau)..time(\tau')]$ となるような乙によるある監査点αが存在しないという仮定は誤りであり、$time(\alpha) \in [time(\tau)..time(\tau')]$ となる乙によるある監査点αが存在する。

【０３２４】

（場合２）τより左に位置する乙による監査点が存在しない場合を考える。このとき、$time(\alpha 0) \in [0..T]$なる監査点$\alpha 0$について、

$\alpha 0 \in [\tau..\tau']$

となることが示される。

【０３２５】

(2) 上述の順次集約木の性質2 と項目(1)から直ちに導かれる。

【０３２６】

(3) τより前に乙の監査点が存在するか否かにより場合分けする。

【０３２７】

（場合1）τより前に乙の監査点が存在する場合を考える。τより前で，最も後に位置する監査点をαとし、 その次の監査点の時刻をα'とする。このとき、

$time(\alpha) < time(\tau) \leqq time(\alpha')$

従って、条件(*2)より、

$time(\alpha') - time(\tau) < time(\alpha') - time(\alpha) \leqq T$

よって、

$time(\alpha') < time(\tau) + T$

以上より、(*4)が得られる。

【０３２８】

（場合２）τより前に乙の監査点が存在しない場合を考える。性質3の前提により、乙の監査点α0でtime(α0) ＜Tとなるものがある。

【０３２９】

time(τ)≦time(α0) ＜ T

従って、

time(α0) － time(τ) ＜ T－ time(τ) ≦ T

よって、time(α0) ＜ time(τ) ＋T

以上により、α' ＝ α0 として、(*4)が得られる。

【０３３０】

(4) 乙の監査点α0で、time(α0) ∈[0..T)となるものが存在するという上記仮定(*1)から、直ちに導かれる。

【０３３１】

（順次集約木の性質4）

SBTを高さkの順次集約木とし、iをSBTの順次集約木リーフ番号とし、k1 ≦ k とし、authPathT$_{k1}$(i)を、authPathT(i)の最初の k1個の要素の列とする。

【０３３２】

authPathT$_{k1}$(i) ＝ [((0, i(0)), LR(0)), …, ((k1－1, i(k1－1)), LR(k1－1))]

と置く。さらにここで、v1, v2 を異なる２つのハッシュ値とし、AP1, AP2 を次のように与える。

【０３３３】

AP1 ＝

[(LR(0), v1'(0)), (LR(1), v1'(1)), …, (LR(k1－1), v1'(k1－1))],

AP2 ＝

[(LR(0), v2'(0)), (LR(1), v2'(1)), …, (LR(k1－1), v2'(k1－1))].

このとき、v1 とAP1 から以下の(*1)ようにに計算した v1''(k1) と、v2 と AP2 から以下の(*2)のように計算した v2''(k1) は（実用上無視できる確率を除いて）一致しない。

【０３３４】

(*1) 各j'∈[0..k1] に対して，v1''(j') を以下のように再帰的に定める。

【０３３５】

v1''(0) ＝ v1。

【０３３６】

j' ＞ 0 で LR(j'－1) ＝ L のとき、

v1''(j') ＝ h(v1'(j'－1)‖v1''(j'－1))

j' ＞ 0 で LR(j'－1) ＝ R のとき、

v1''(j') ＝ h(v1''(j'－1)‖v1'(j'－1))

(*2) 各j'∈[0..k] に対して、v2''(j') を以下のように再帰的に定める。

【０３３７】

v2''(0) ＝ v2

j' ＞ 0 で LR(j'－1) ＝ L のとき、

v2''(j') ＝ h(v2'(j'－1)‖v2''(j'－1))

j' ＞ 0 で LR(j'－1) ＝ R のとき、

v2''(j') ＝ h(v2''.(j'－1)‖v2'(j'－1))

・性質4の証明

v1''(k1) ＝ v2''(k1) と仮定する。j' ∈[0..k1] で v1''(j') ＝ v2''(j') となる最小のj' をj1 と置く。v1≠v2、 即ち v1''(0) ≠ v2''(0) であるから、j1 ＞ 0 である。j0 ＝ j1 － 1 と置く。LR(j0) が L であるか R であるかにより場合分けする。

【０３３８】

（場合1）LR(j0) ＝ L のとき。j1, j0のとり方より、

v1''(j0) ≠ v2''(j0)。

【０３３９】

従って、

v1'(j0)‖v1''(j0) ≠ v2'(j0)‖v2''(j0)

一方、上述の(*1)，(*2) から、

v1''(j1) ＝ h(v1'(j0)‖v1''(j0))

v2''(j1) ＝ h(v2'(j0)‖v2''(j0))

従って、

h(v1'(j0)‖v1''(j0)) ＝ h(v2'(j0)‖v2''(j0))

従って、v1'(j0)‖v1''(j0)とv2'(j0)‖v2''(j0)が、衝突困難ハッシュ関数 hの衝突となる。

【０３４０】

（場合２） LR(j0) ＝ R のとき、場合１に於けると同様にして、

v1''(j0)‖v1'(j0)とv2''(j0)‖v2'(j0)が，衝突困難ハッシュ関数 hの衝突となることが導かれる。

【０３４１】

以上から、どちらの場合でも，衝突困難ハッシュ関数 hの衝突が現れることになる。このようなことは（実用上無視できる確率を除いて）在り得ない。従って、 v1''(k) ＝ v2''(k)となることも、（実用上無視できる確率を除いて）在り得ない。

【図面の簡単な説明】

【０３４２】

【図１】本発明の第１の実施の形態に係るイベント順序証明システムのシステム構成図である。

【図２】本発明の第１の実施の形態に係るイベント順序証明システムの別のシステム構成図である。

【図３】本発明に用いられる順次集約木の構成を説明する図である。

【図４】本発明におけるイベント順序受理証明書の構成を説明する図である。

【図５】本発明に用いられる順次集約木の認証パスを説明する図である。

【図６】本発明の第１の実施の形態に係るイベント順序証明システムのイベント順序証明方法を説明するシーケンス図である。

【図７】本発明の第１の実施の形態に係るイベント順序証明システムのイベント順序証明検証方法を説明するシーケンス図である。

【図８】本発明の第１の実施の形態に係るイベント順序証明システムのイベント順序証明検証方法を説明するシーケンス図である。

【図９】本発明の第１の実施の形態に係るイベント順序証明システムにおけるユーザ点と監査点の関係を説明する図である。

【図１０】本発明の第１の実施の形態に係るイベント順序証明システムのイベント順序証明検証結果を説明する図である。

【図１１】本発明の第２の実施の形態に係るイベント順序証明システムのシステム構成図である。

【図１２】本発明の第２の実施の形態に係るイベント順序証明システムにおけるユーザ点と監査点の関係を説明する図である。

【図１３】本発明の第２の実施の形態に係るイベント順序証明システムのイベント順序証明方法を説明するシーケンス図である。

【図１４】本発明の第２の実施の形態に係るイベント順序証明システムのイベント順序証明検証方法を説明するシーケンス図である。

【図１５】本発明の第２の実施の形態に係るイベント順序証明システムの２ユーザ間の順序を判定する動作を説明するフローチャート図である。

【図１６】本発明の第２の実施の形態に係るイベント順序証明システムの複合完全化によるルート値検証の動作を説明するフローチャート図である。

【図１７】本発明の第２の実施の形態に係るイベント順序証明システムの補完データ完全化を説明する図である。
【図１８】本発明の第２の実施の形態に係るイベント順序証明システムの補完データ完全化を説明する図である。
【図１９】本発明の第３の実施の形態に係るイベント順序証明システムのシステム構成図である。
【図２０】本発明の第３の実施の形態に係るイベント順序証明システムのイベント順序証明方法のイベント順序証明要求ステップを説明するシーケンス図である。
【図２１】本発明の第３の実施の形態に係るイベント順序証明システムのイベント順序証明方法のイベント順序証明要求ステップを説明するシーケンス図である。
【図２２】本発明の第３の実施の形態に係るイベント順序証明システムのイベント順序証明方法の監査用受理証明書受信ステップを説明するシーケンス図である。
【図２３】本発明の第３の実施の形態に係るイベント順序証明システムのイベント順序証明検証方法の区間時刻証明書ステップを説明するシーケンス図である。
【図２４】深さの違いを１以内に押さえ、ダミーノードを作成しない動的な順次集約木の構成方法を説明する図である。
【図２５】インクリメンタルに順次集約木を構成する方法のアルゴリズムを説明する図である。
【図２６】インクリメンタルに順次集約木を構成する方法のアルゴリズムを説明する図である。
【図２７】インクリメンタルに順次集約木を構成する方法を説明する図である。
【図２８】インクリメンタルに順次集約木を構成する方法において各ノードに値を割付けるタイミングを説明する図である。
【図２９】認証点の割当値は、監査点の受理証明書内補完データに含まれることを説明する図である。
【図３０】認証点のレベルより低い認証パスノードは、遅延補完データあるいは受理証明書内補完データに含まれることを説明する図である。
【図３１】認証点のレベルより低い認証パスノードは、遅延補完データあるいは受理証明書内補完データに含まれることを説明する図である。
【図３２】イベント順序証明システムの概念を説明する図である。
【図３３】線形リンキングを用いたイベント順序証明システムの概念を説明する図である。

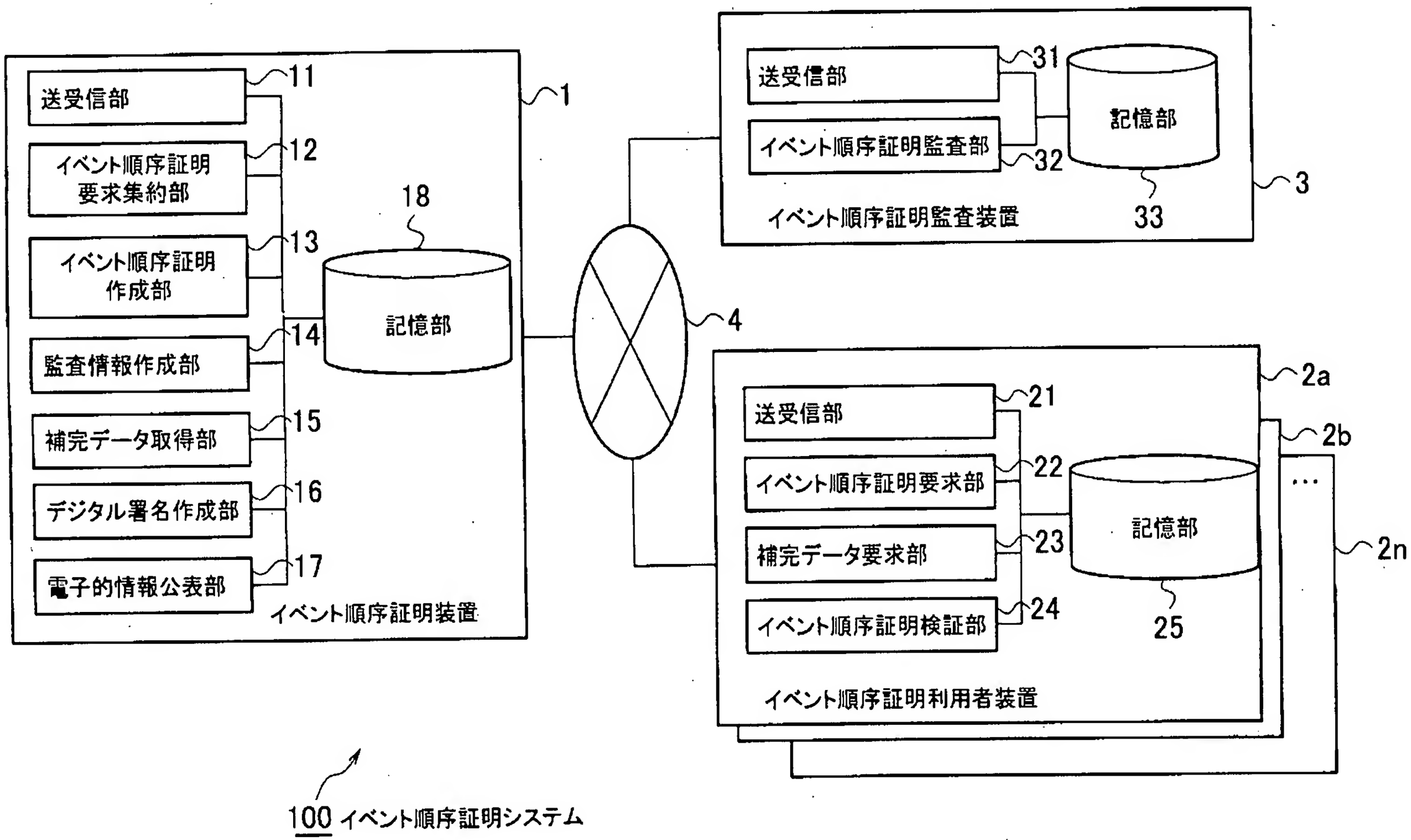
【符号の説明】

【０３４３】

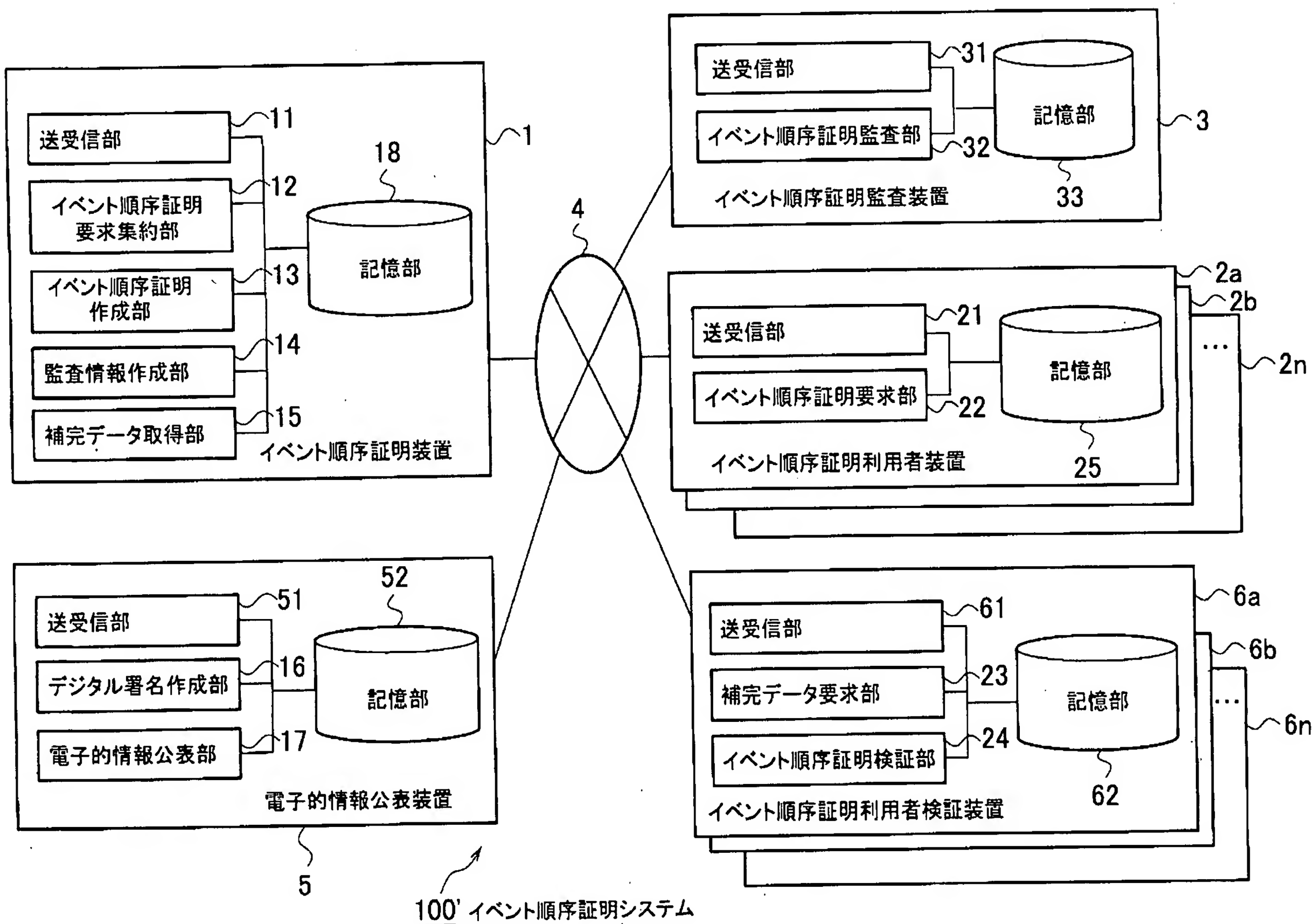
１，７，９０…イベント順序証明装置
２ｉ…イベント順序証明利用者装置
３，８…イベント順序証明監査装置
４…コンピュータネットワーク
５…電子的情報公表装置
６…イベント順序証明利用者検証装置
９…イベント順序証明監査装置＆イベント時刻監査装置
１０ｊ…時刻証明利用者装置
１１，２１，３１，５１，６１…送受信部
１２…イベント順序証明要求部
１３…イベント順序証明作成部
１４，７１…監査情報作成部
１５…補完データ取得部
１６…デジタル署名作成部
１７…電子的情報公表部
１８，２５，３３，５２，６２，７２，８３，９２，２０４…記憶部

２０ｉ…イベント順序証明利用者装置＆時刻証明装置
２２，２０２…イベント順序証明要求部
２３…補完データ要求部
２４，２０３…イベント順序証明検証部
３０…時刻情報提供装置
３２，８２…イベント順序証明監査部
８０…利用者
８１…補完データ要求部
９１…区間時刻証明証作成部
１００，２００，３００，９００，９１０…イベント順序証明システム
２０１…時刻証明作成部

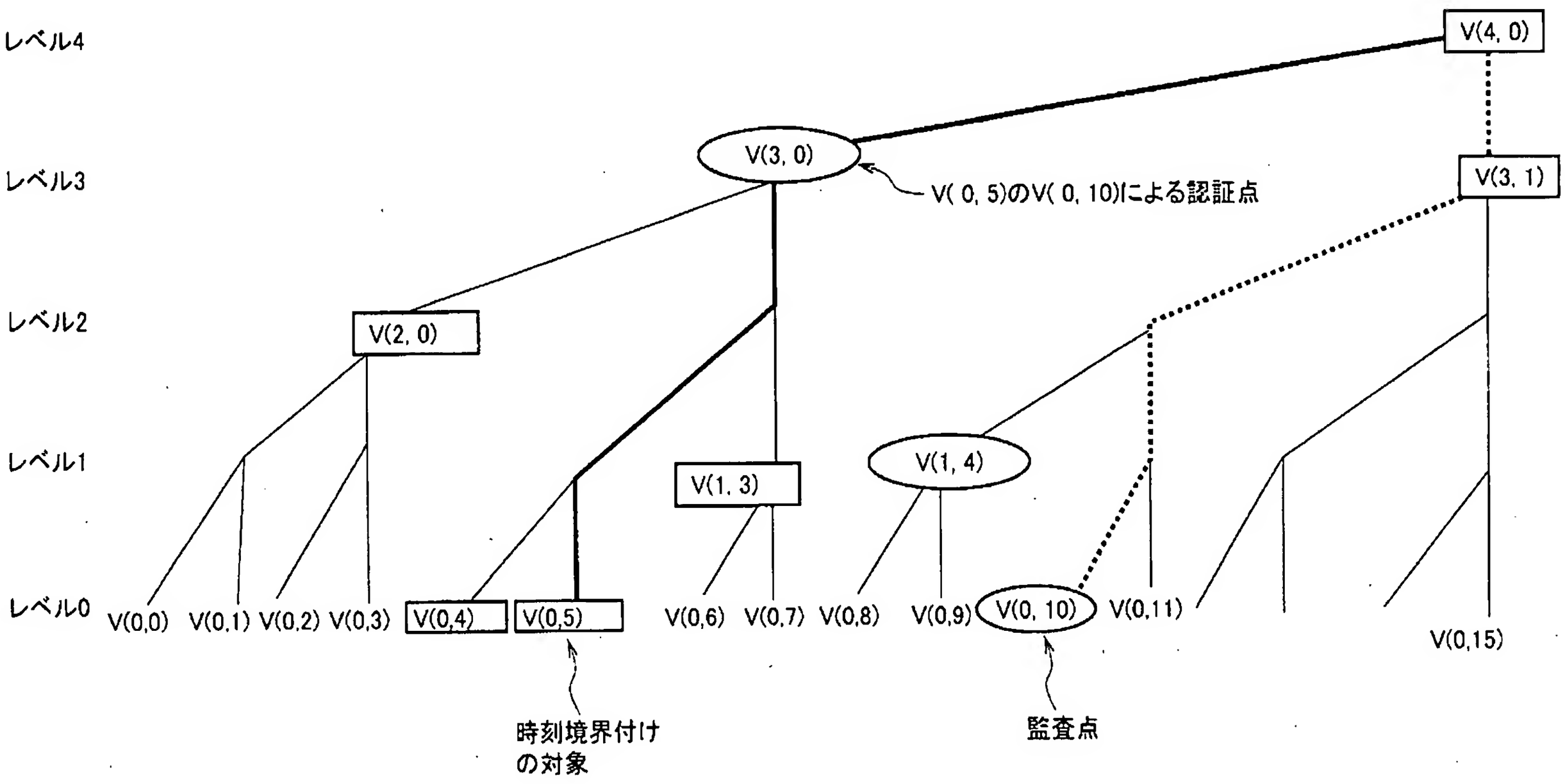
【書類名】 図面
【図１】


送受信部
11
イベント順序証明
要求集約部
12
イベント順序証明
作成部
13
監査情報作成部
14
補完データ取得部
15
デジタル署名作成部
16
電子的情報公表部
17
18
記憶部
イベント順序証明装置
1
4
送受信部
31
イベント順序証明監査部
32
記憶部
33
イベント順序証明監査装置
3
2a
2b
2n
送受信部
21
イベント順序証明要求部
22
補完データ要求部
23
イベント順序証明検証部
24
記憶部
25
イベント順序証明利用者装置
100 イベント順序証明システム

【図２】


送受信部
11
イベント順序証明
要求集約部
12
イベント順序証明
作成部
13
監査情報作成部
14
補完データ取得部
15
18
記憶部
イベント順序証明装置
1
4
送受信部
31
イベント順序証明監査部
32
記憶部
33
イベント順序証明監査装置
3
2a
2b
2n
送受信部
21
イベント順序証明要求部
22
記憶部
25
イベント順序証明利用者装置
送受信部
51
デジタル署名作成部
16
電子的情報公表部
17
52
記憶部
電子的情報公表装置
5
6a
6b
6n
送受信部
61
補完データ要求部
23
イベント順序証明検証部
24
記憶部
62
イベント順序証明利用者検証装置
100'
イベント順序証明システム

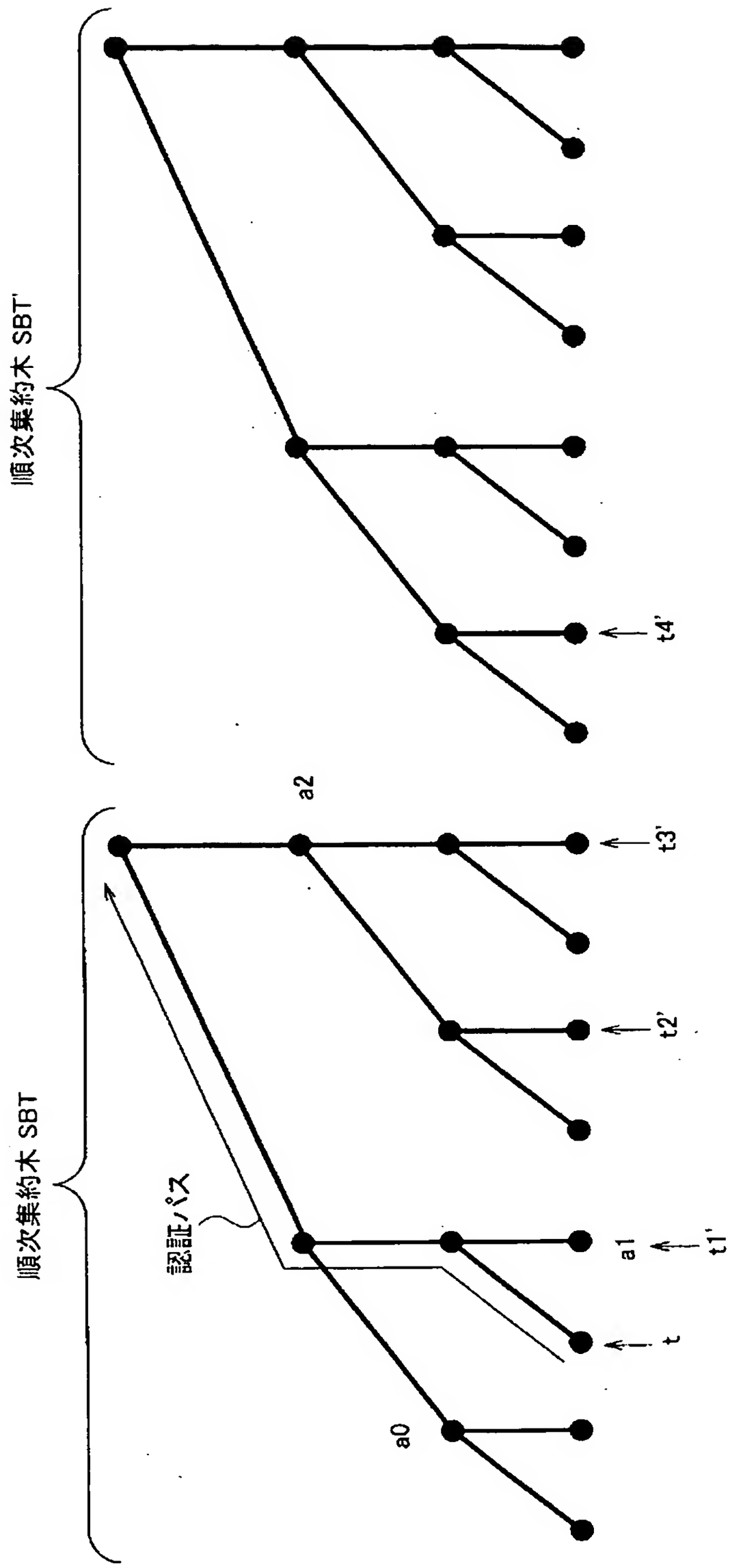
【図３】


レベル4
レベル3
レベル2
レベル1
レベル0
V(4, 0)
V(3, 0)
V(3, 1)
V(0, 5)のV(0, 10)による認証点
V(2, 0)
V(1, 3)
V(1, 4)
V(0,0)
V(0,1)
V(0,2)
V(0,3)
V(0,4)
V(0,5)
V(0,6)
V(0,7)
V(0,8)
V(0,9)
V(0, 10)
V(0,11)
V(0,15)
時刻境界付け
の対象
監査点

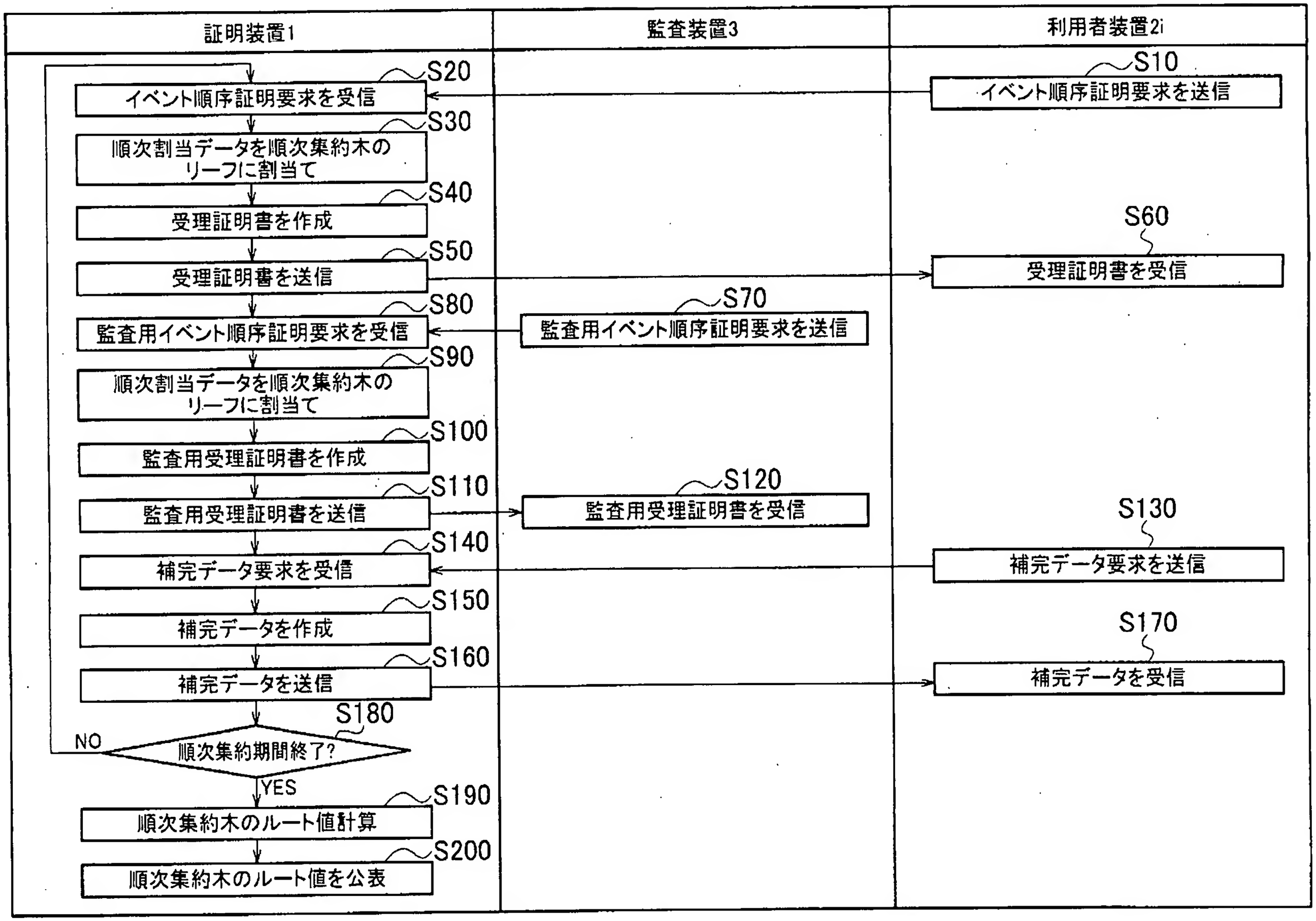
【図４】

項目	記号	必須
元デジタルデータ	y	○
順次割当データ	z	○
順次集約木番号	n	○
順次集約木リーフ番号	i	○
即時補完データ(位置情報、割当値)	HK	
デジタル署名	DS	

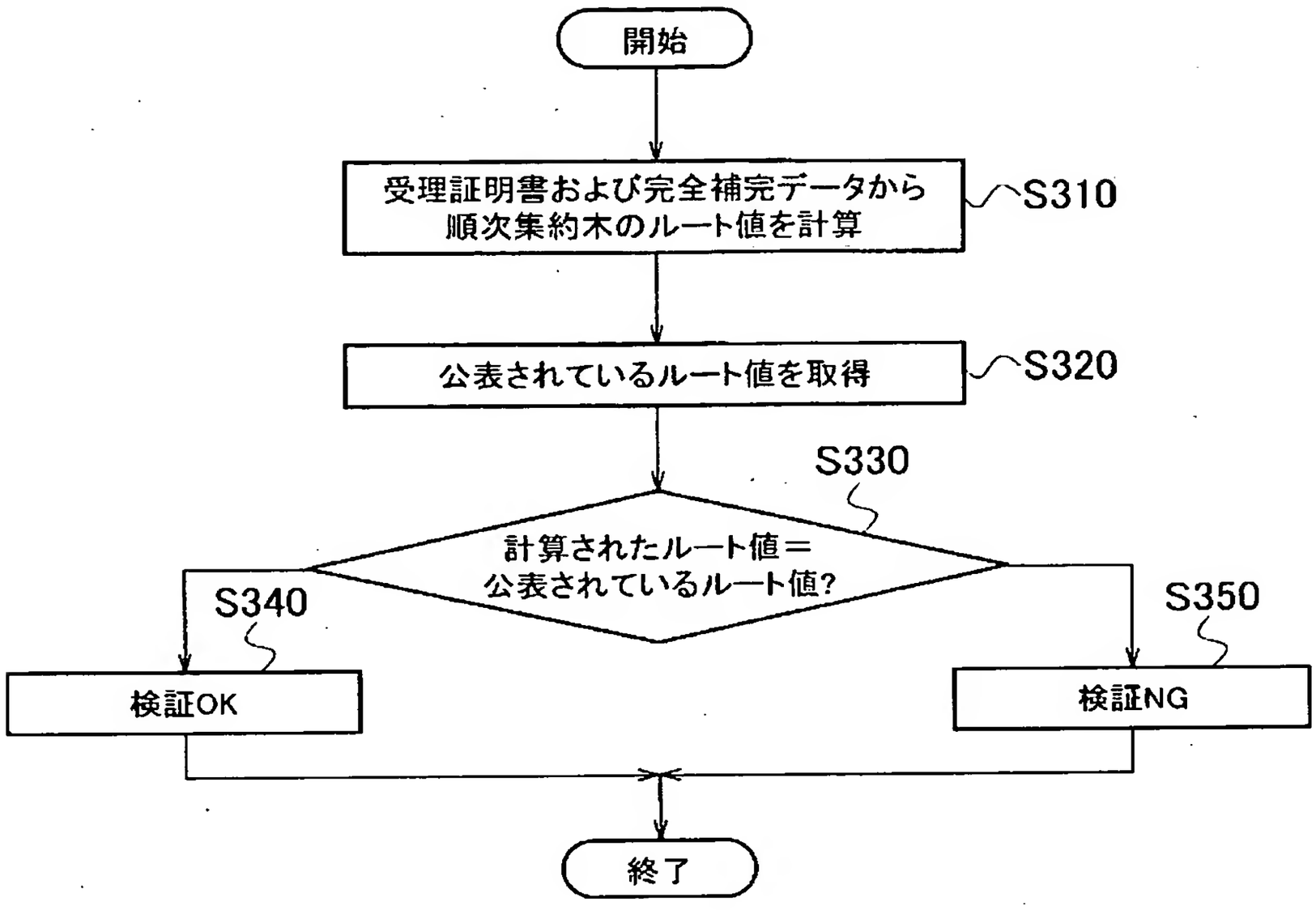
【図５】



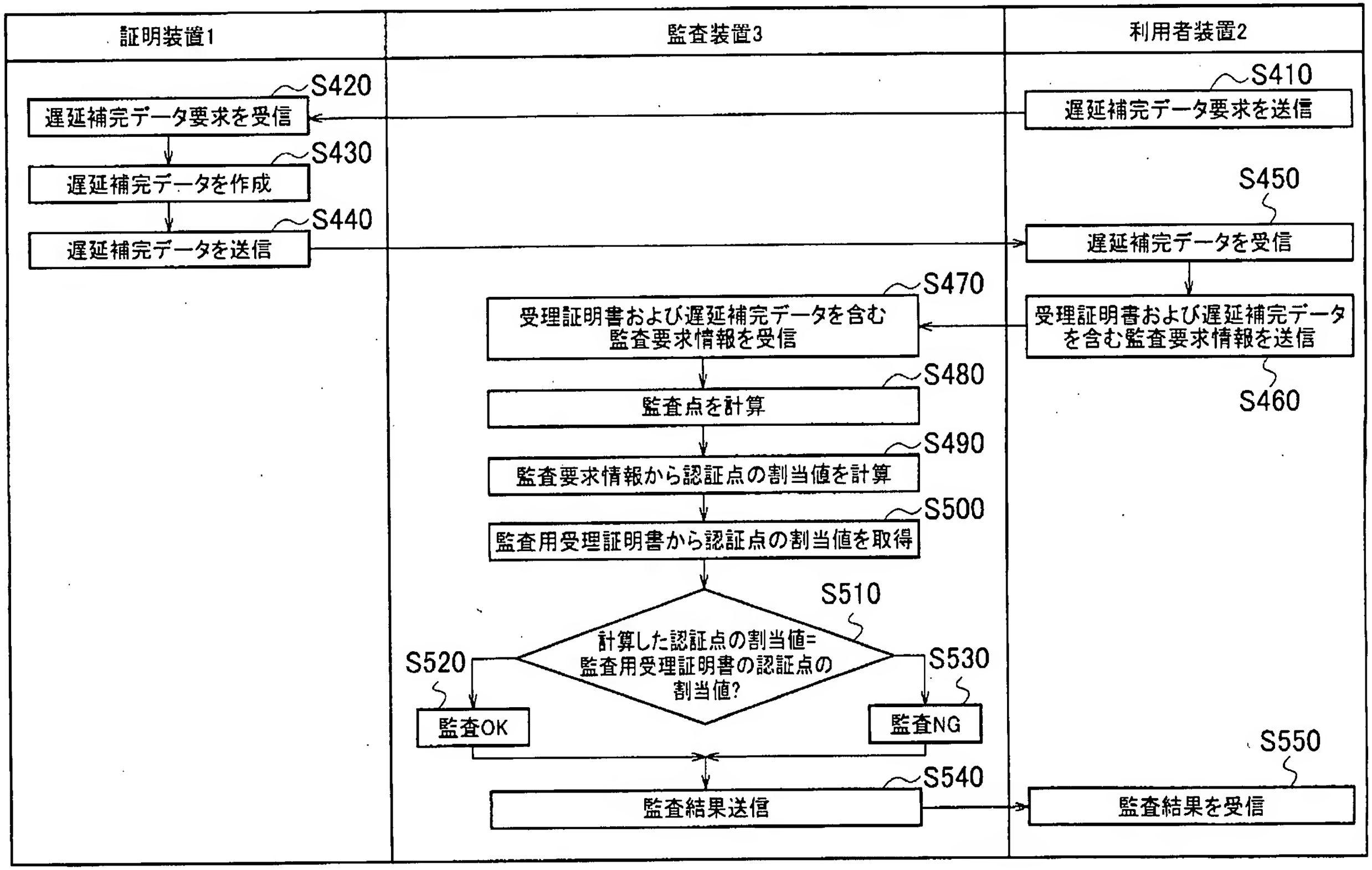
【図６】


証明装置1
監査装置3
利用者装置2i
S10
イベント順序証明要求を送信
S20
イベント順序証明要求を受信
S30
順次割当データを順次集約木のリーフに割当て
S40
受理証明書を作成
S50
受理証明書を送信
S60
受理証明書を受信
S70
監査用イベント順序証明要求を送信
S80
監査用イベント順序証明要求を受信
S90
順次割当データを順次集約木のリーフに割当て
S100
監査用受理証明書を作成
S110
監査用受理証明書を送信
S120
監査用受理証明書を受信
S130
補完データ要求を送信
S140
補完データ要求を受信
S150
補完データを作成
S160
補完データを送信
S170
補完データを受信
S180
順次集約期間終了?
NO
YES
S190
順次集約木のルート値計算
S200
順次集約木のルート値を公表

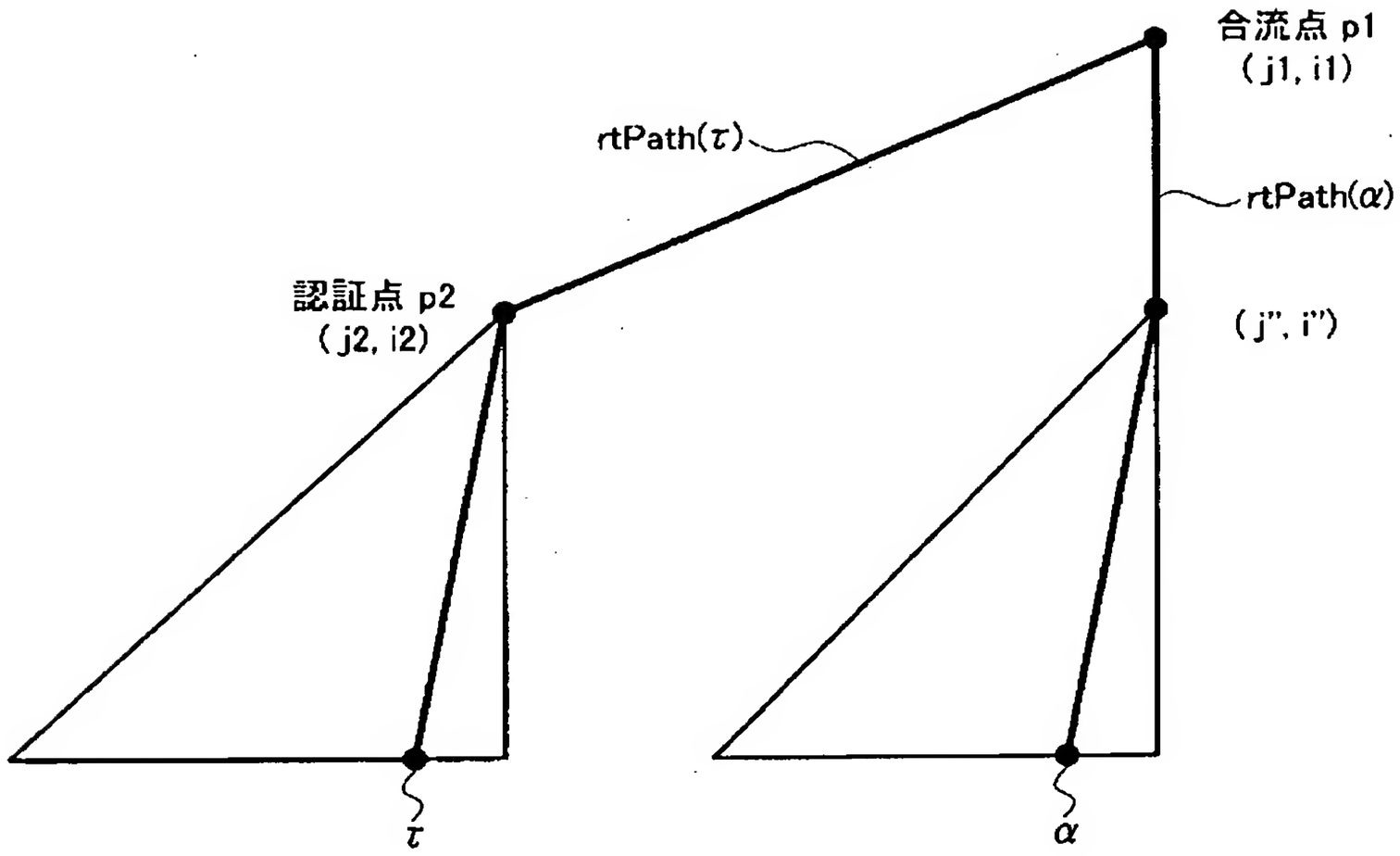
【図７】


開始
受理証明書および完全補完データから
順次集約木のルート値を計算
S310
公表されているルート値を取得
S320
S330
計算されたルート値＝
公表されているルート値?
S340
検証OK
S350
検証NG
終了

【図８】


証明装置1
監査装置3
利用者装置2
S410
遅延補完データ要求を送信
S420
遅延補完データ要求を受信
S430
遅延補完データを作成
S440
遅延補完データを送信
S450
遅延補完データを受信
S460
受理証明書および遅延補完データを含む監査要求情報を送信
S470
受理証明書および遅延補完データを含む監査要求情報を受信
S480
監査点を計算
S490
監査要求情報から認証点の割当値を計算
S500
監査用受理証明書から認証点の割当値を取得
S510
計算した認証点の割当値=監査用受理証明書の認証点の割当値?
S520
監査OK
S530
監査NG
S540
監査結果送信
S550
監査結果を受信

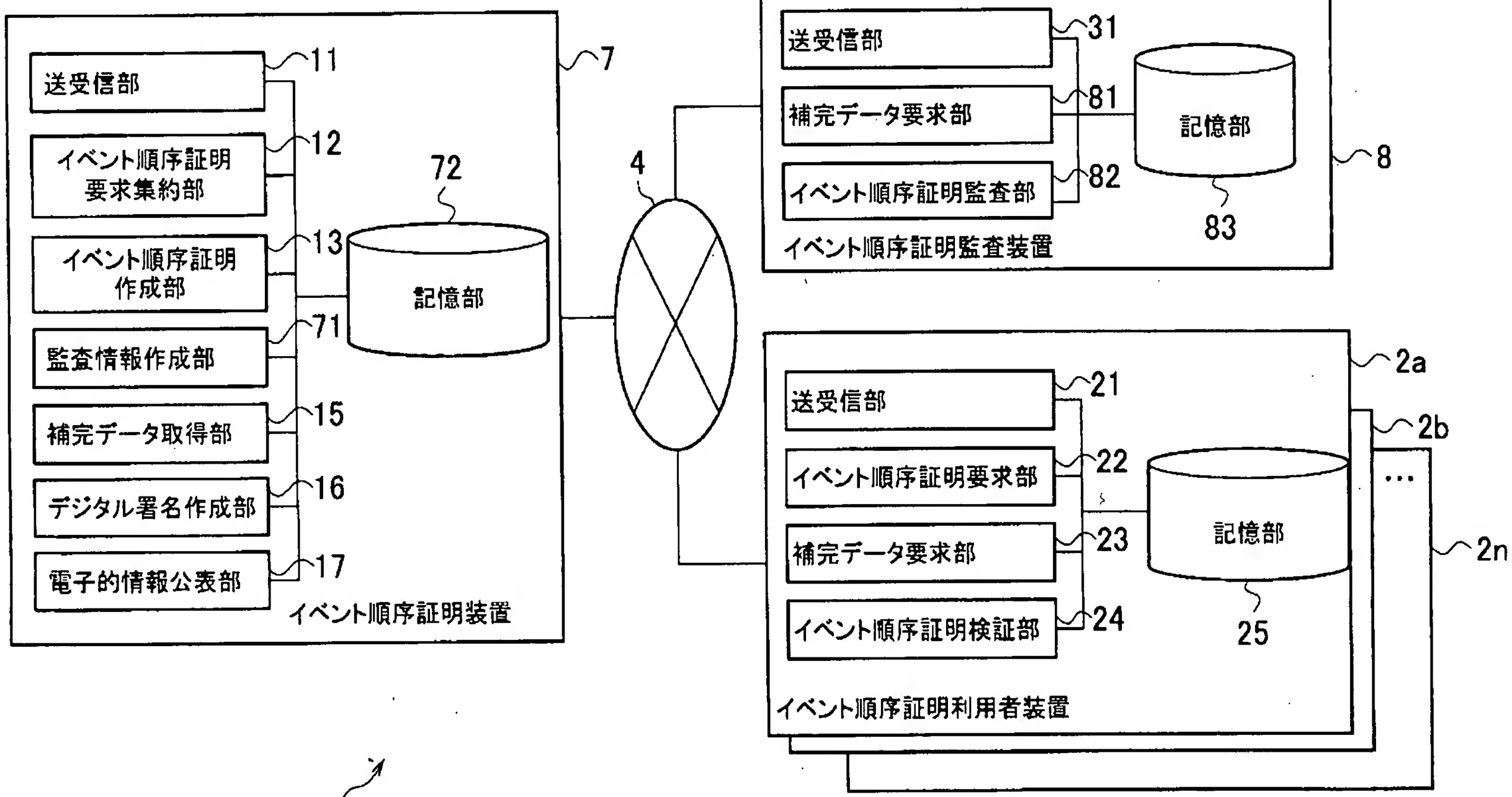
【図９】



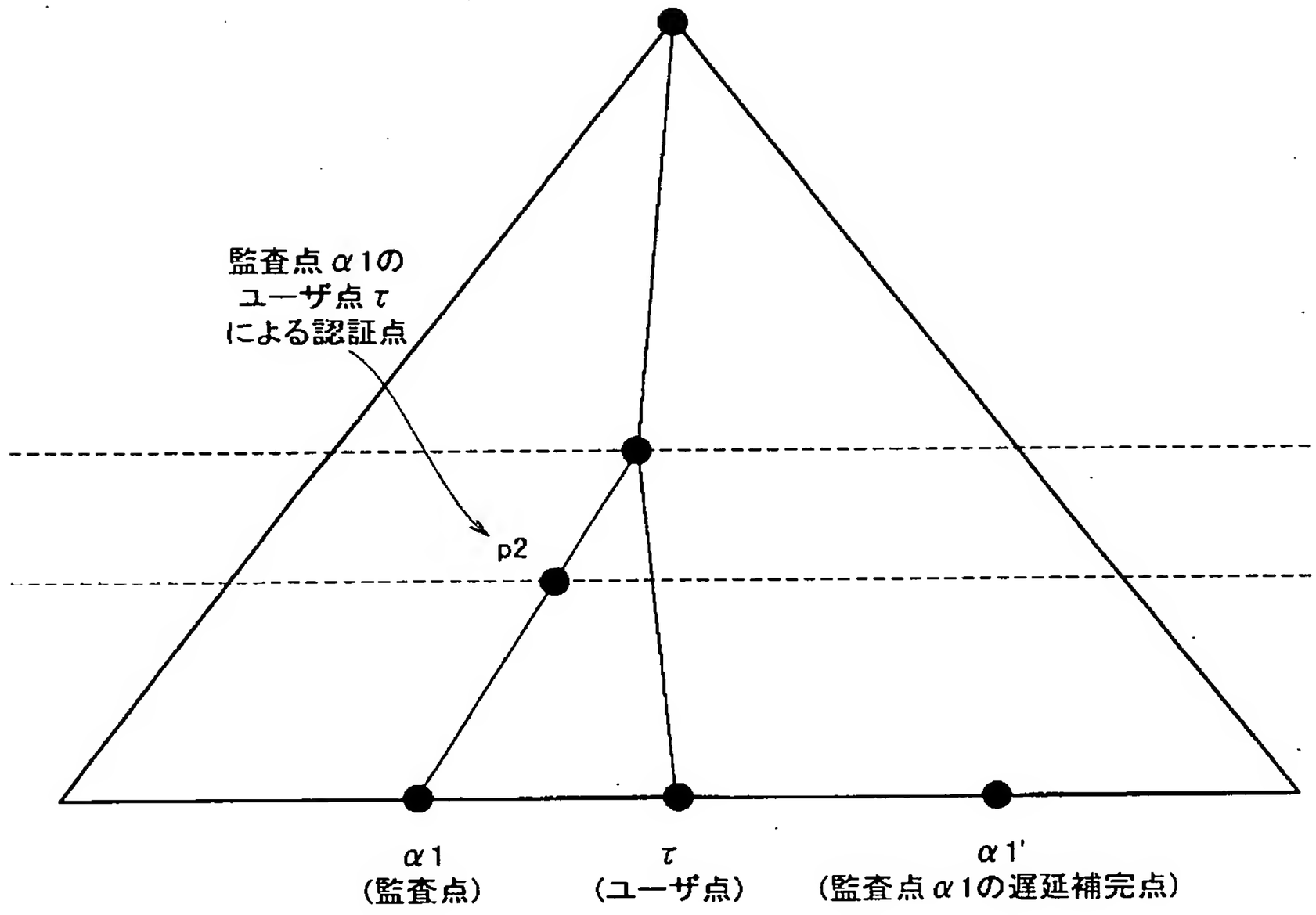
【図１０】

検証結果1	証明装置1 証明要求の受信時点 (ユーザ点τに対応) 監査用受理証明書の送信時点 (監査点αに対応) 時間t
検証結果2	証明装置1 証明要求の受信時点 (ユーザ点τに対応) 監査用証明受付の受信時点 (監査点αに対応) 時間t

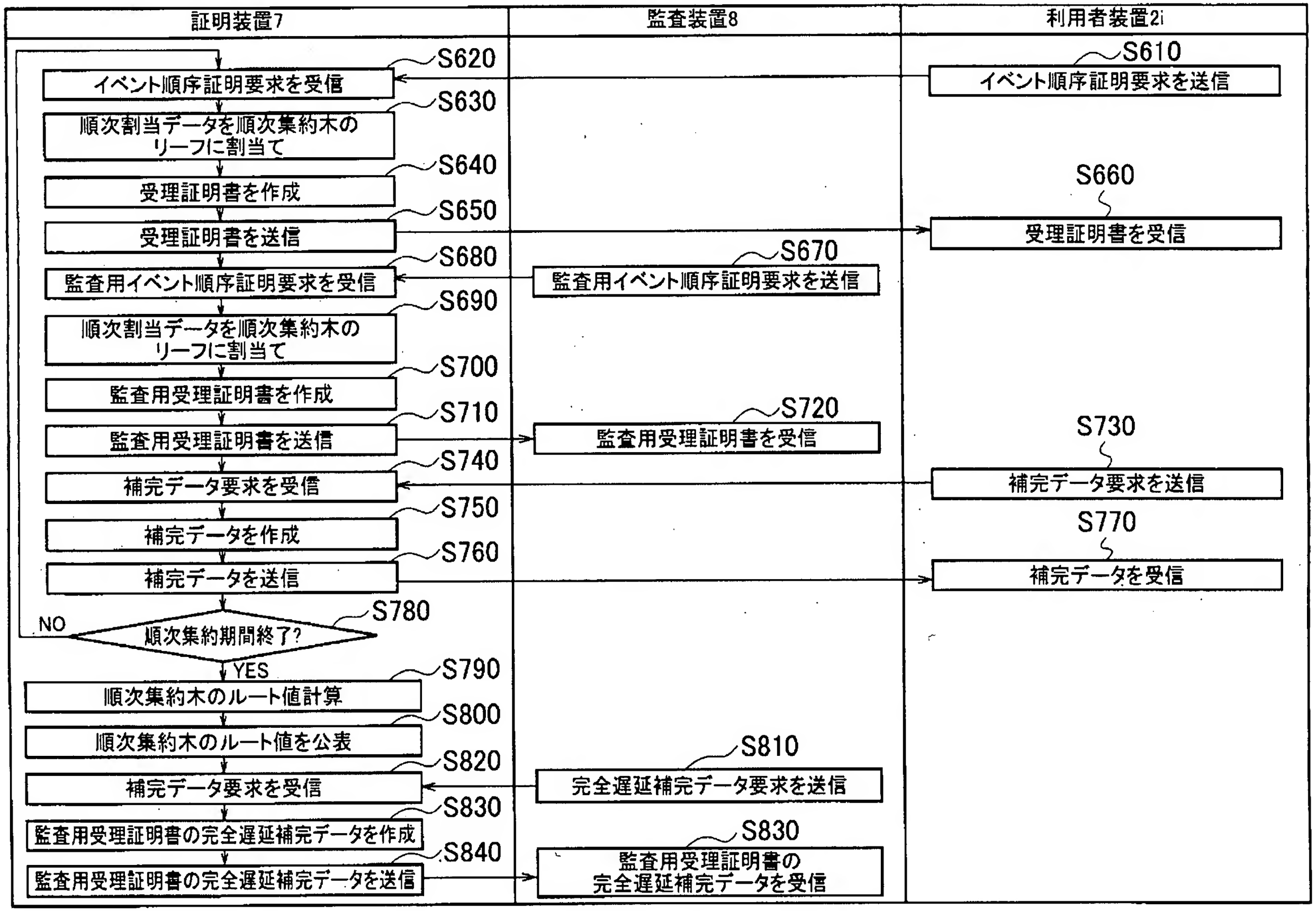
【図１１】


送受信部
11
イベント順序証明
要求集約部
12
イベント順序証明
作成部
13
監査情報作成部
71
補完データ取得部
15
デジタル署名作成部
16
電子的情報公表部
17
72
記憶部
7
イベント順序証明装置
4
送受信部
31
補完データ要求部
81
イベント順序証明監査部
82
記憶部
83
8
イベント順序証明監査装置
送受信部
21
イベント順序証明要求部
22
補完データ要求部
23
イベント順序証明検証部
24
記憶部
25
2a
2b
2n
イベント順序証明利用者装置
200 イベント順序証明システム

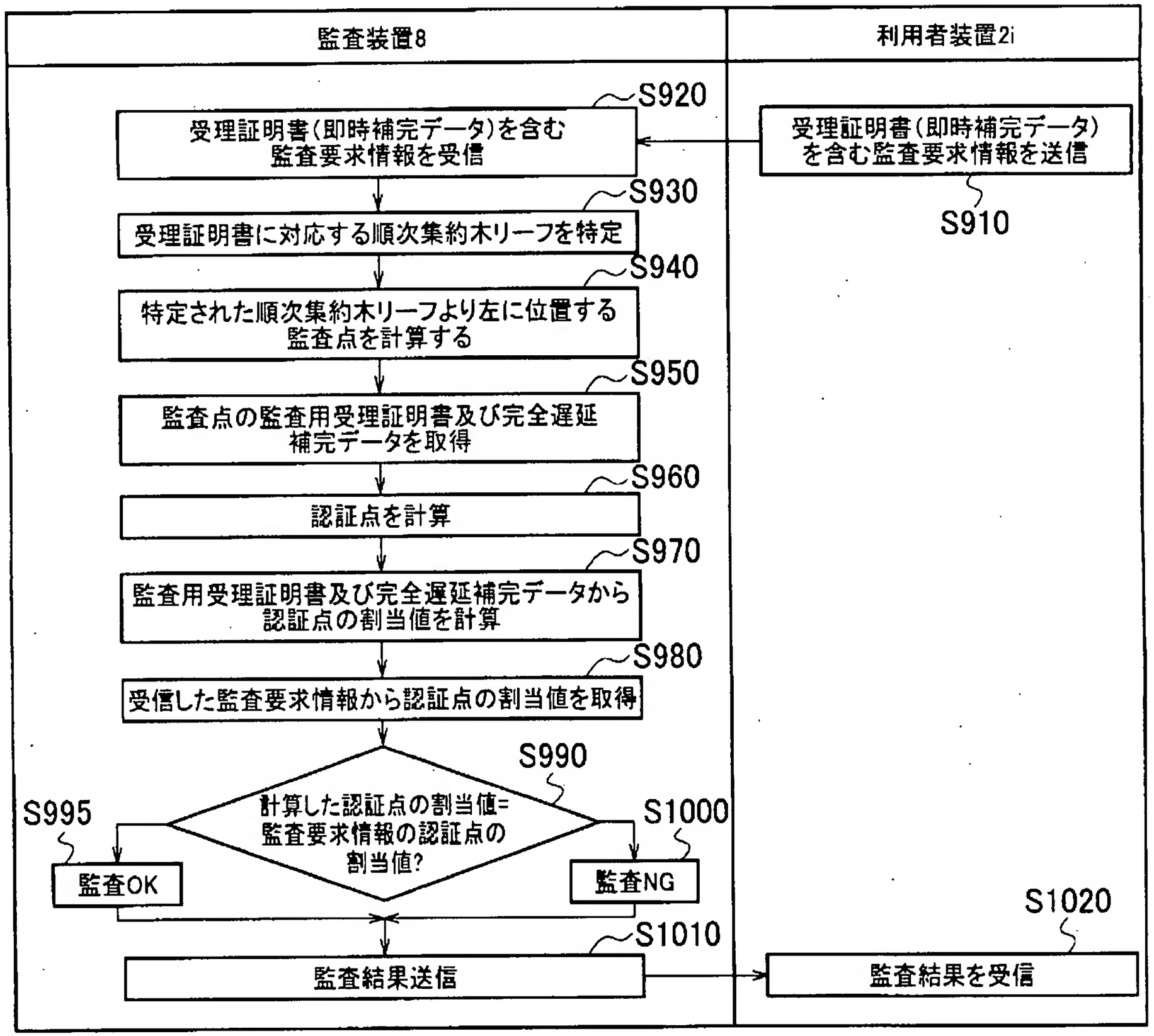
【図１２】



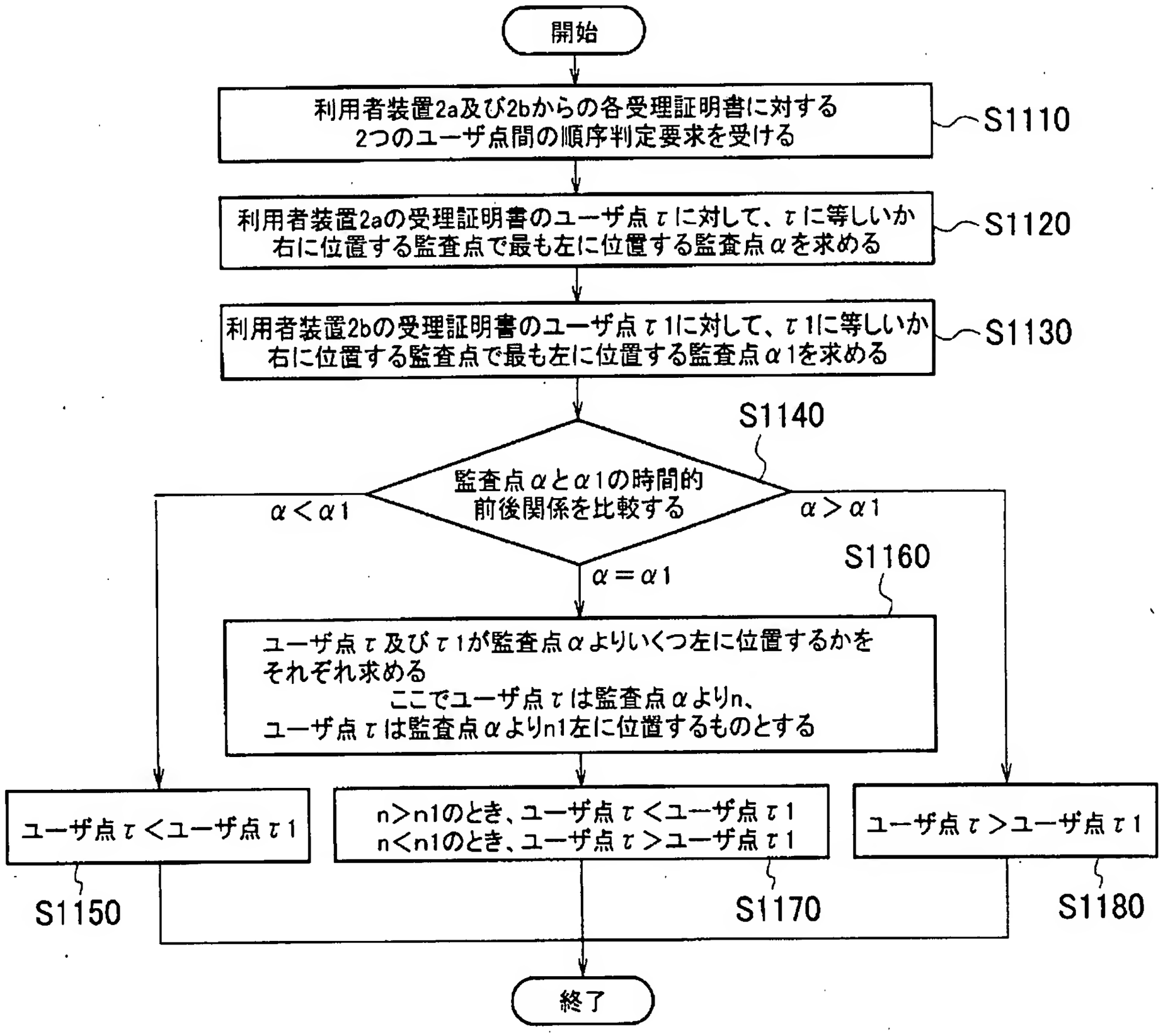
【図１３】


証明装置7
監査装置8
利用者装置2i
S620
イベント順序証明要求を受信
S610
イベント順序証明要求を送信
S630
順次割当データを順次集約木のリーフに割当て
S640
受理証明書を作成
S650
受理証明書を送信
S660
受理証明書を受信
S680
監査用イベント順序証明要求を受信
S670
監査用イベント順序証明要求を送信
S690
順次割当データを順次集約木のリーフに割当て
S700
監査用受理証明書を作成
S710
監査用受理証明書を送信
S720
監査用受理証明書を受信
S730
補完データ要求を送信
S740
補完データ要求を受信
S750
補完データを作成
S760
補完データを送信
S770
補完データを受信
S780
順次集約期間終了?
NO
YES
S790
順次集約木のルート値計算
S800
順次集約木のルート値を公表
S810
完全遅延補完データ要求を送信
S820
補完データ要求を受信
S830
監査用受理証明書の完全遅延補完データを作成
S830
監査用受理証明書の完全遅延補完データを受信
S840
監査用受理証明書の完全遅延補完データを送信

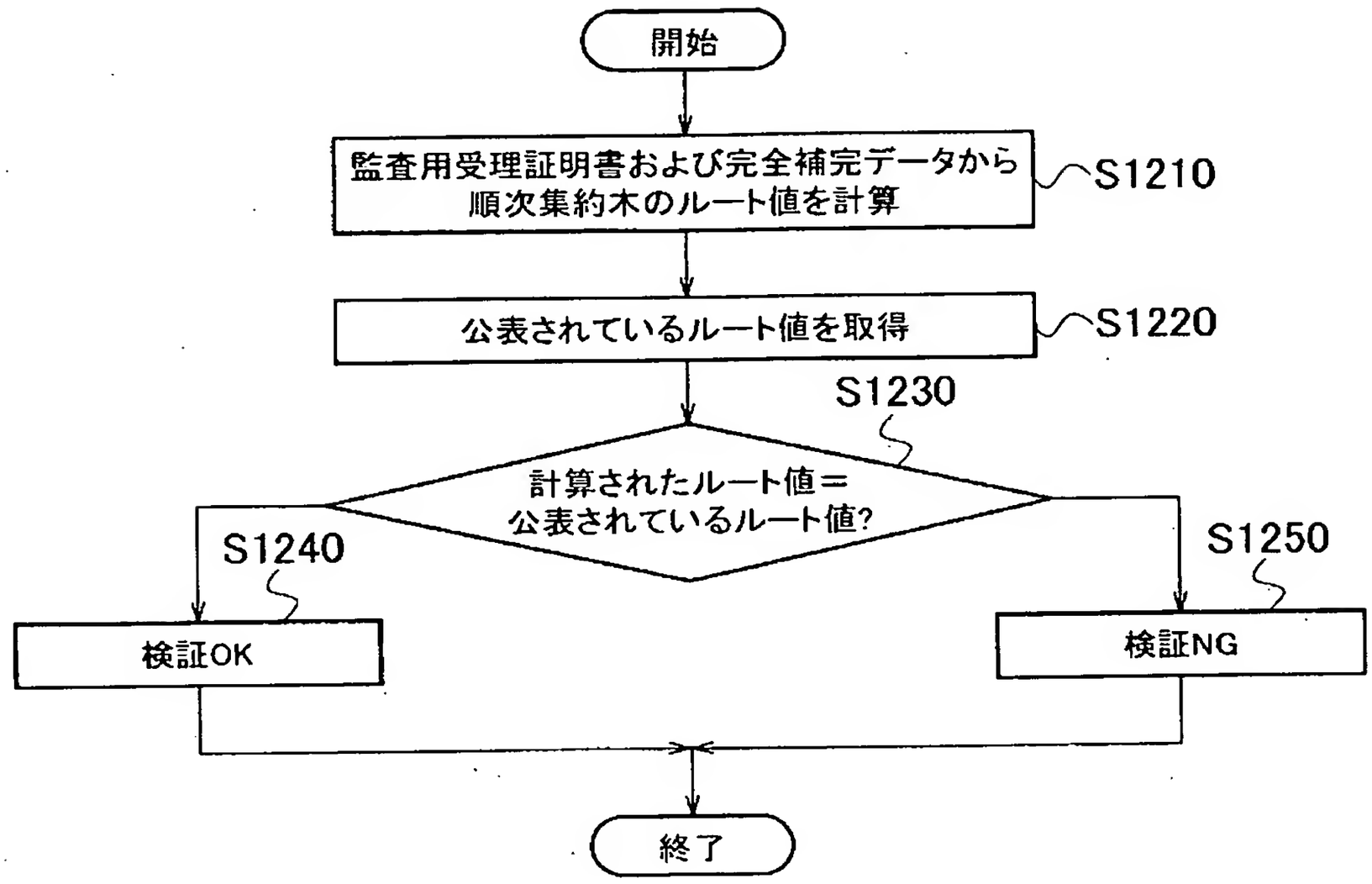
【図１４】


監査装置8
利用者装置2i
S920
受理証明書(即時補完データ)を含む
監査要求情報を受信
受理証明書(即時補完データ)
を含む監査要求情報を送信
S910
S930
受理証明書に対応する順次集約木リーフを特定
S940
特定された順次集約木リーフより左に位置する
監査点を計算する
S950
監査点の監査用受理証明書及び完全遅延
補完データを取得
S960
認証点を計算
S970
監査用受理証明書及び完全遅延補完データから
認証点の割当値を計算
S980
受信した監査要求情報から認証点の割当値を取得
S990
計算した認証点の割当値=
監査要求情報の認証点の
割当値?
S995
監査OK
S1000
監査NG
S1010
監査結果送信
S1020
監査結果を受信

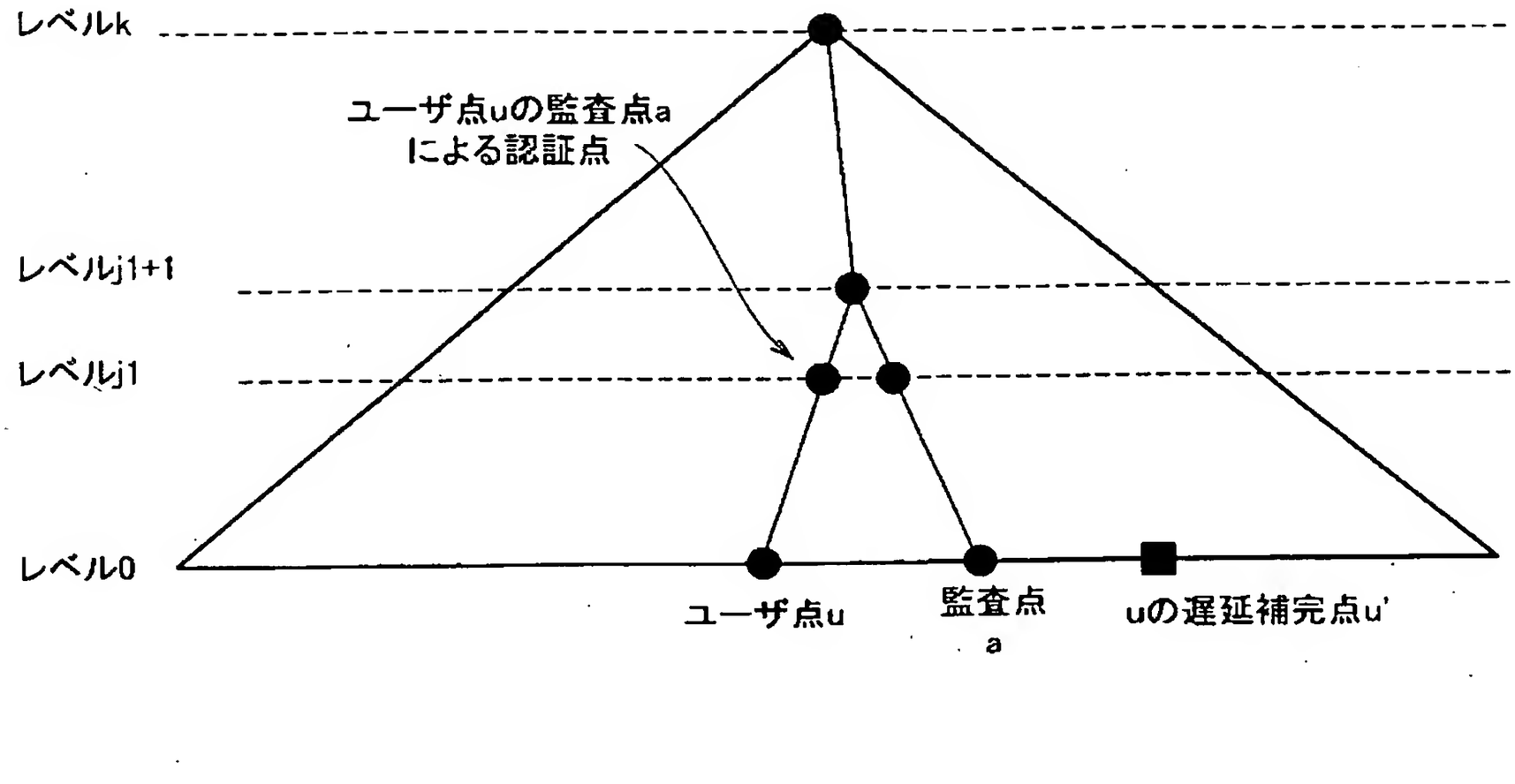
【図１５】


開始
利用者装置2a及び2bからの各受理証明書に対する
2つのユーザ点間の順序判定要求を受ける
S1110
利用者装置2aの受理証明書のユーザ点τに対して、τに等しいか
右に位置する監査点で最も左に位置する監査点αを求める
S1120
利用者装置2bの受理証明書のユーザ点τ1に対して、τ1に等しいか
右に位置する監査点で最も左に位置する監査点α1を求める
S1130
S1140
監査点αとα1の時間的
前後関係を比較する
α＜α1
α＝α1
α＞α1
S1160
ユーザ点τ及びτ1が監査点αよりいくつ左に位置するかを
それぞれ求める
ここでユーザ点τは監査点αよりn、
ユーザ点τは監査点αよりn1左に位置するものとする
ユーザ点τ＜ユーザ点τ1
S1150
n＞n1のとき、ユーザ点τ＜ユーザ点τ1
n＜n1のとき、ユーザ点τ＞ユーザ点τ1
S1170
ユーザ点τ＞ユーザ点τ1
S1180
終了

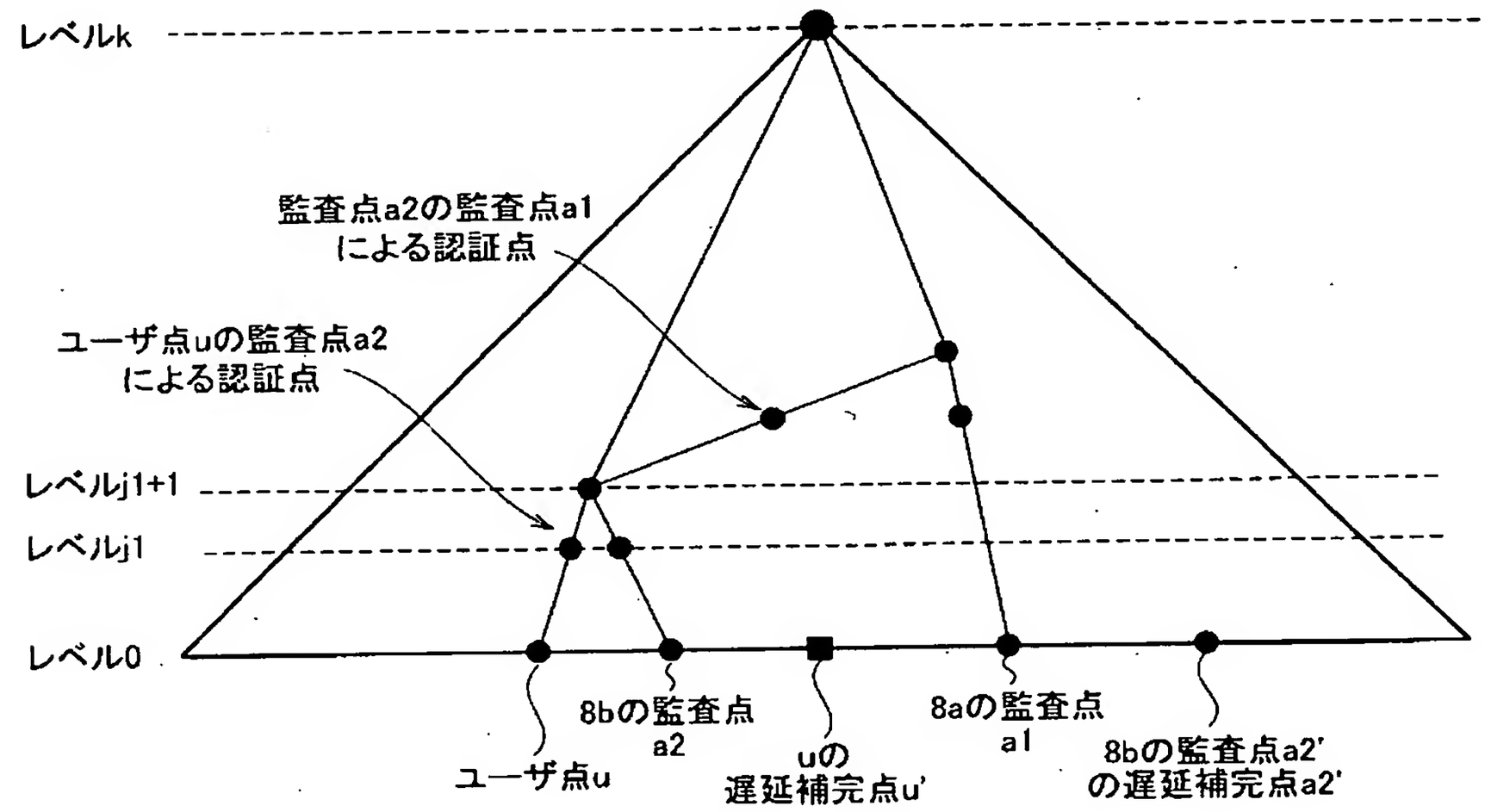
【図１６】


開始
監査用受理証明書および完全補完データから順次集約木のルート値を計算
S1210
公表されているルート値を取得
S1220
S1230
計算されたルート値＝公表されているルート値?
S1240
検証OK
S1250
検証NG
終了

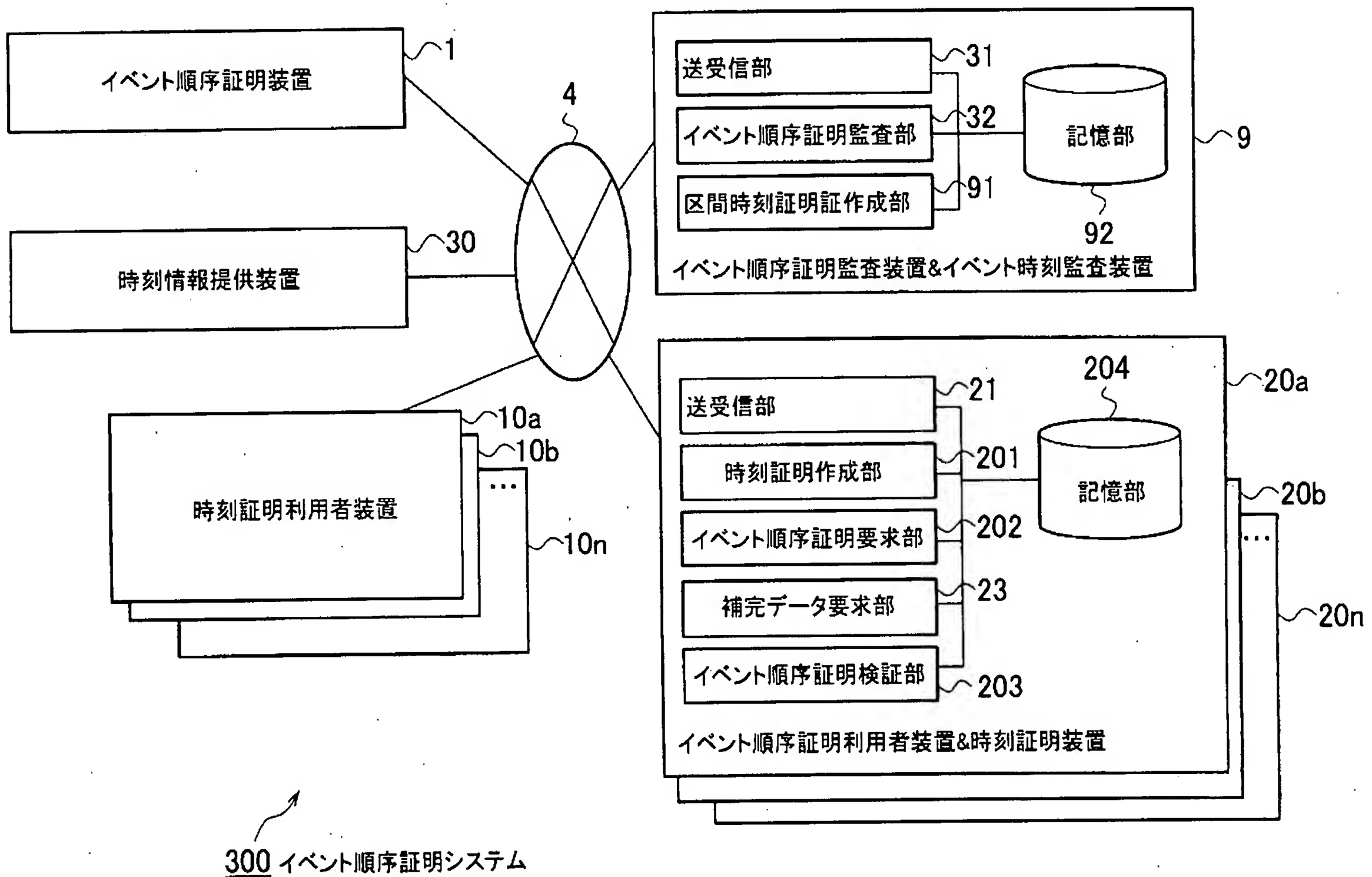
【図１７】


レベルk
ユーザ点uの監査点a
による認証点
レベルj1+1
レベルj1
レベル0
ユーザ点u
監査点
a
uの遅延補完点u'

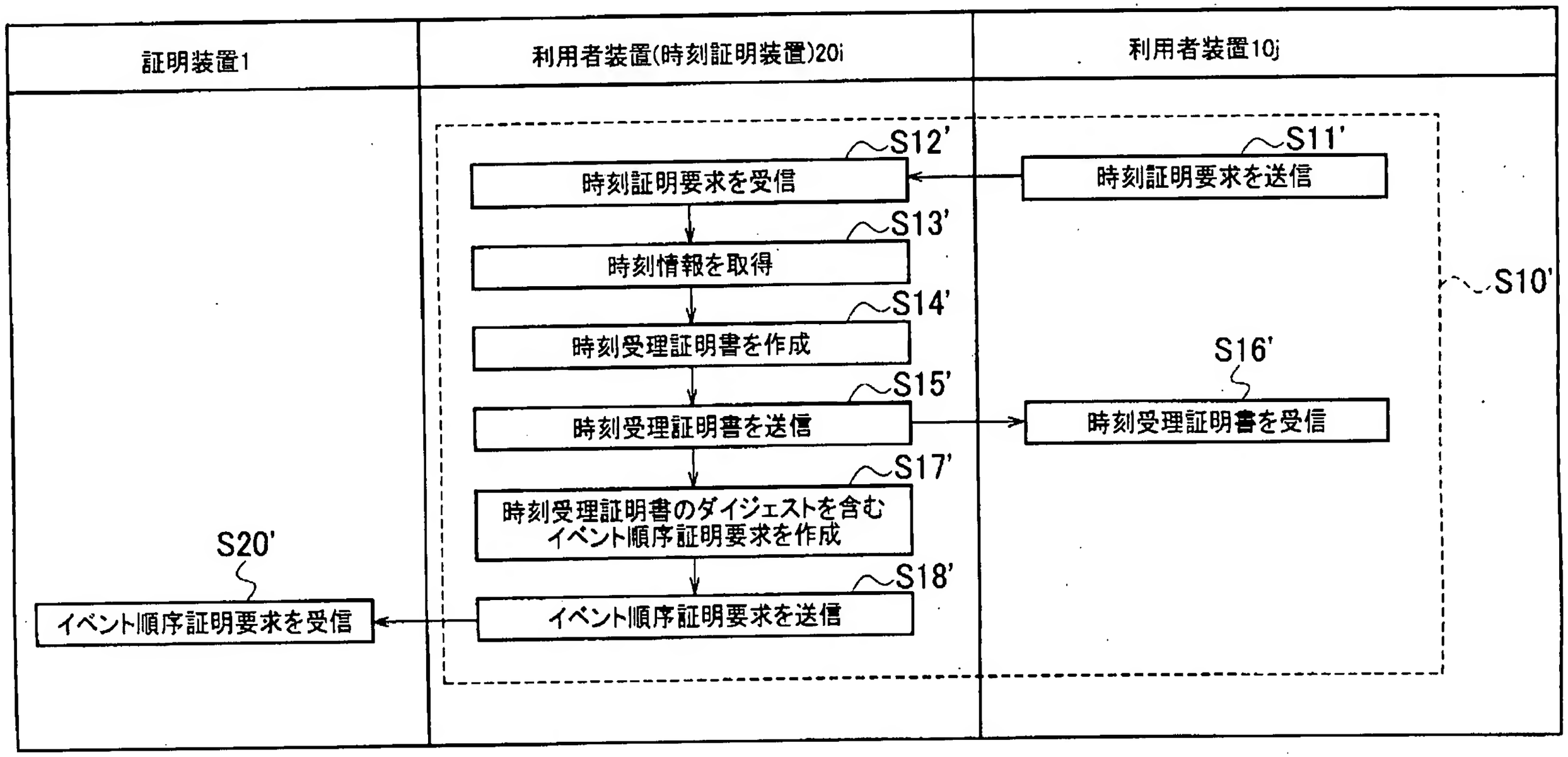
【図１８】


レベルk
監査点a2の監査点a1
による認証点
ユーザ点uの監査点a2
による認証点
レベルj1+1
レベルj1
レベル0
8bの監査点
a2
ユーザ点u
uの
遅延補完点u'
8aの監査点
a1
8bの監査点a2'
の遅延補完点a2'

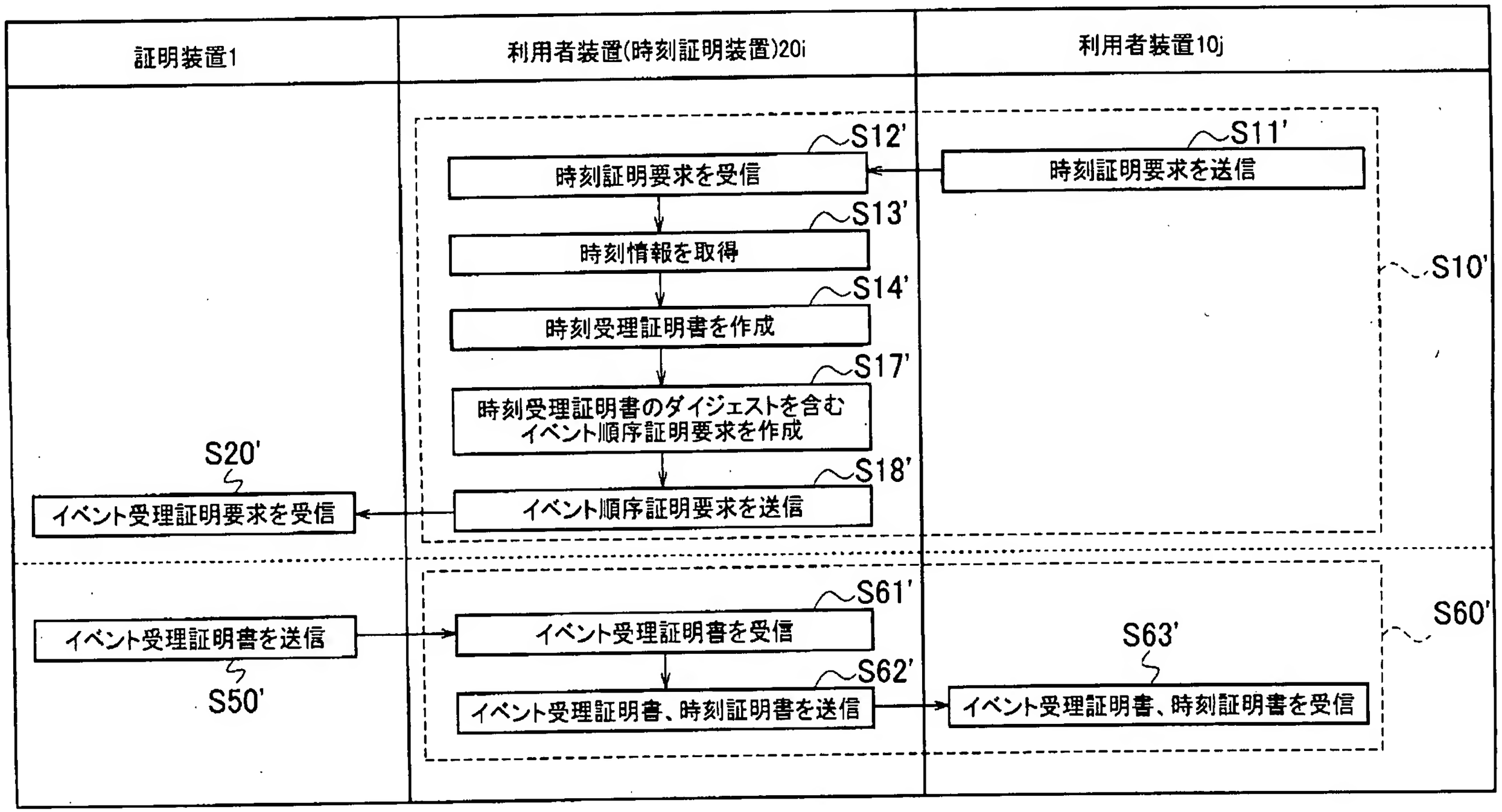
【図１９】


イベント順序証明装置
1
時刻情報提供装置
30
4
送受信部
31
イベント順序証明監査部
32
区間時刻証明証作成部
91
記憶部
92
9
イベント順序証明監査装置&イベント時刻監査装置
10a
10b
10n
時刻証明利用者装置
204
20a
送受信部
21
時刻証明作成部
201
記憶部
イベント順序証明要求部
202
補完データ要求部
23
イベント順序証明検証部
203
20b
20n
イベント順序証明利用者装置&時刻証明装置
300 イベント順序証明システム

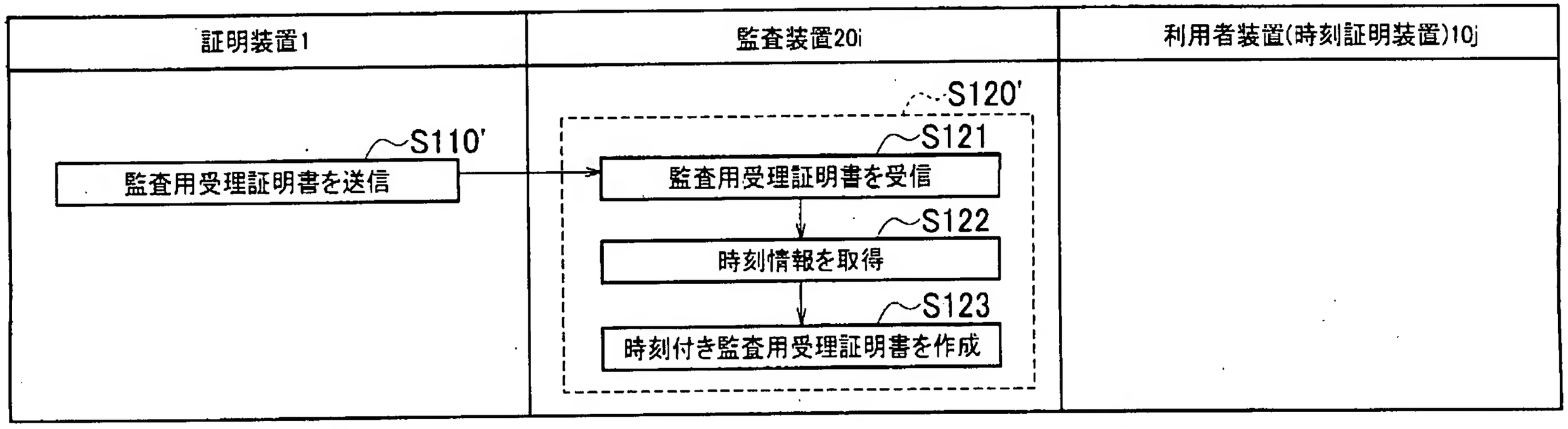
【図２０】


証明装置1
利用者装置(時刻証明装置)20i
利用者装置10j
S10'
S11'
時刻証明要求を送信
S12'
時刻証明要求を受信
S13'
時刻情報を取得
S14'
時刻受理証明書を作成
S15'
時刻受理証明書を送信
S16'
時刻受理証明書を受信
S17'
時刻受理証明書のダイジェストを含む
イベント順序証明要求を作成
S18'
イベント順序証明要求を送信
S20'
イベント順序証明要求を受信

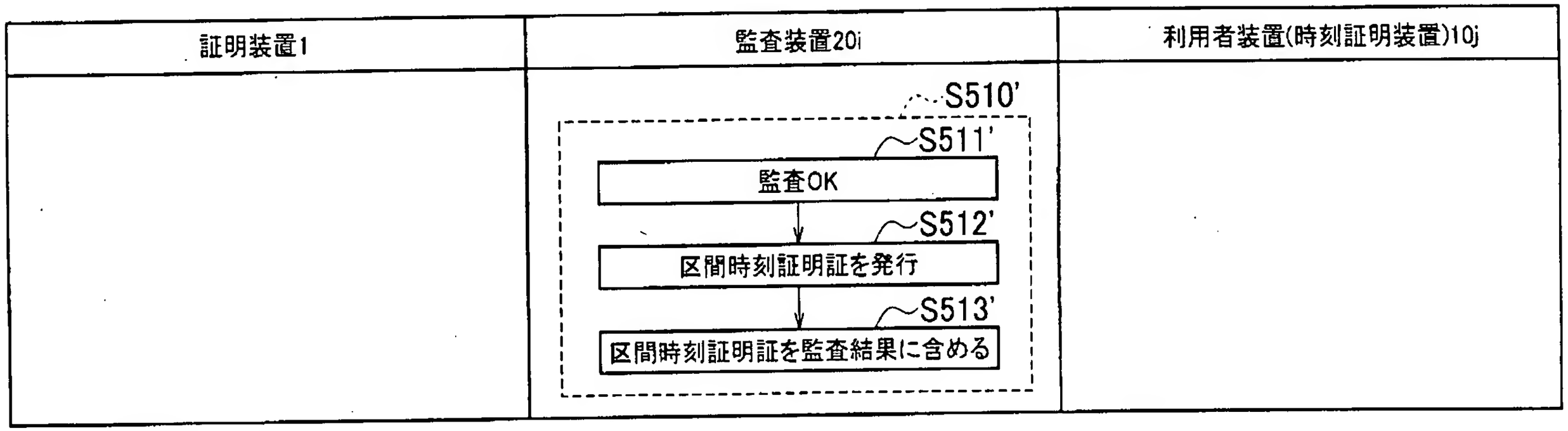
【図２１】


証明装置1
利用者装置(時刻証明装置)20i
利用者装置10j
S12'
時刻証明要求を受信
S11'
時刻証明要求を送信
S13'
時刻情報を取得
S14'
時刻受理証明書を作成
S17'
時刻受理証明書のダイジェストを含む
イベント順序証明要求を作成
S10'
S18'
イベント順序証明要求を送信
S20'
イベント受理証明要求を受信
S61'
イベント受理証明書を受信
S60'
S63'
イベント受理証明書を送信
S62'
イベント受理証明書、時刻証明書を送信
イベント受理証明書、時刻証明書を受信
S50'

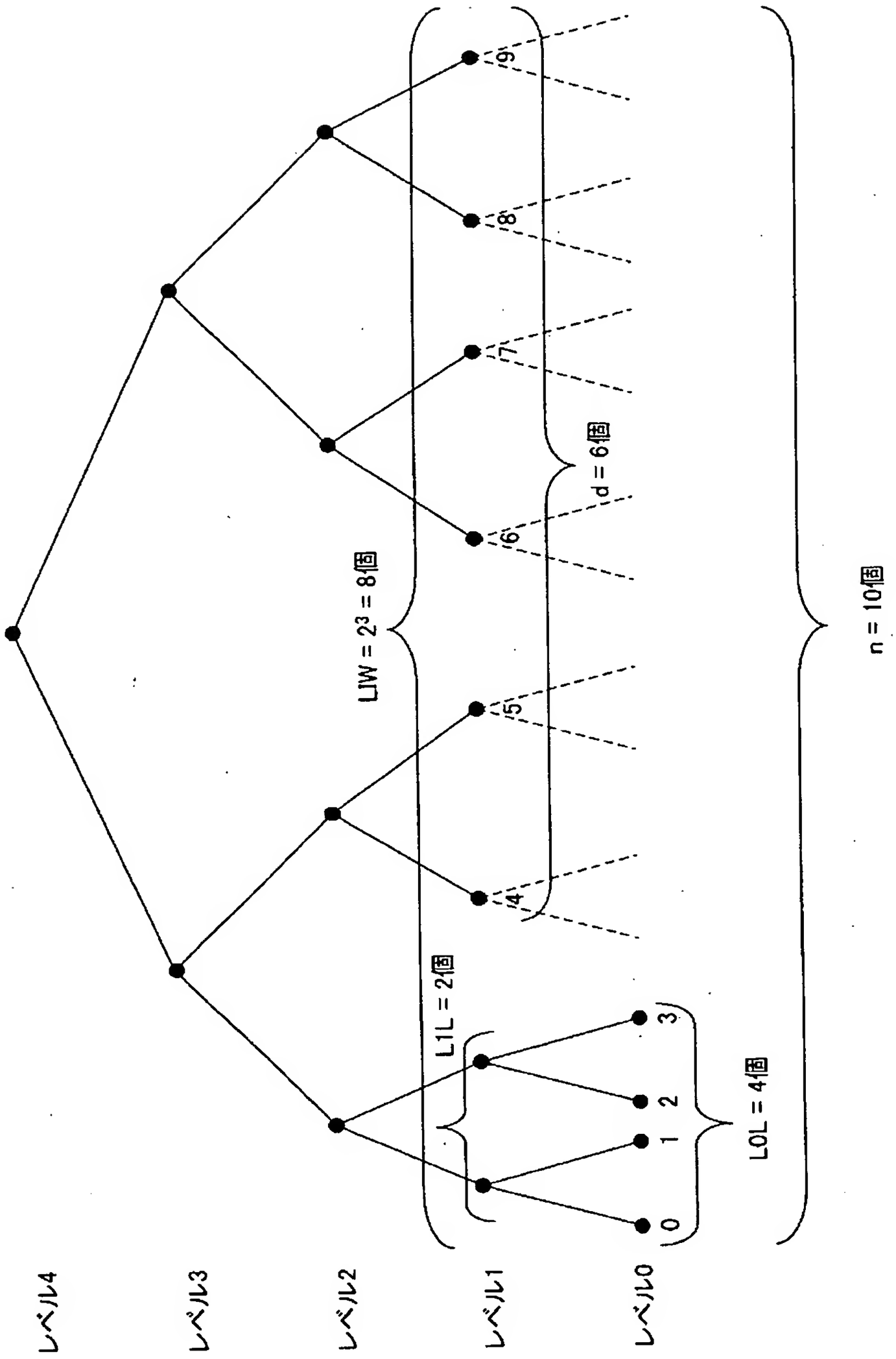
【図２２】


証明装置1
監査装置20i
利用者装置(時刻証明装置)10j
S120'
S110'
監査用受理証明書を送信
S121
監査用受理証明書を受信
S122
時刻情報を取得
S123
時刻付き監査用受理証明書を作成

【図２３】


証明装置1
監査装置20i
利用者装置(時刻証明装置)10j
S510'
S511'
監査OK
S512'
区間時刻証明証を発行
S513'
区間時刻証明証を監査結果に含める

【図２４】


レベル4
レベル3
レベル2
レベル1
レベル0
0
1
2
3
L0L = 4個
L1L = 2個
LIW = 2³ = 8個
n = 10個
d = 6個
4
5
6
7
8
9

【図２５】

(1) ループ1：構成法その3では、定められた時間間隔が終了するまで
以下の処理を繰り返す.

(1.1) 受け付けた要求をxに置く.

(1.2) nを1インクリメントする.

(1.3) ループ2：j = 0, ..., Kに対して以下の処理を行う.

(1.3.1) i : = i_jと置く.

(1.3.2) j = 0のときは、A_j[i] : = x
(即ち、ノード(j, i_j)にxを設定する).

(1.3.3) j ＞ 0のときは、以下を行う.

- x0 : = A_{j-1}[index(leftChiild(j, i))]
(ノード(j, i) のleft-childに割り付けられた値をx0とおく).
- x1 : = A_{j-1}[index(rightChild(j, i))]
(ノード(j, i) のright-childに割り付けられた値をx1とおく).
- x2 : = h(x0 || x1)を計算する.
- A_j[i] : = x2
(即ち、ノード(j, i) にx2を割り付ける).

(1.3.4) i_j を1インクリメントする.

(1.3.5) iが偶数のときは、ループ2を抜ける.

ループ2終了.

ループ1終了.

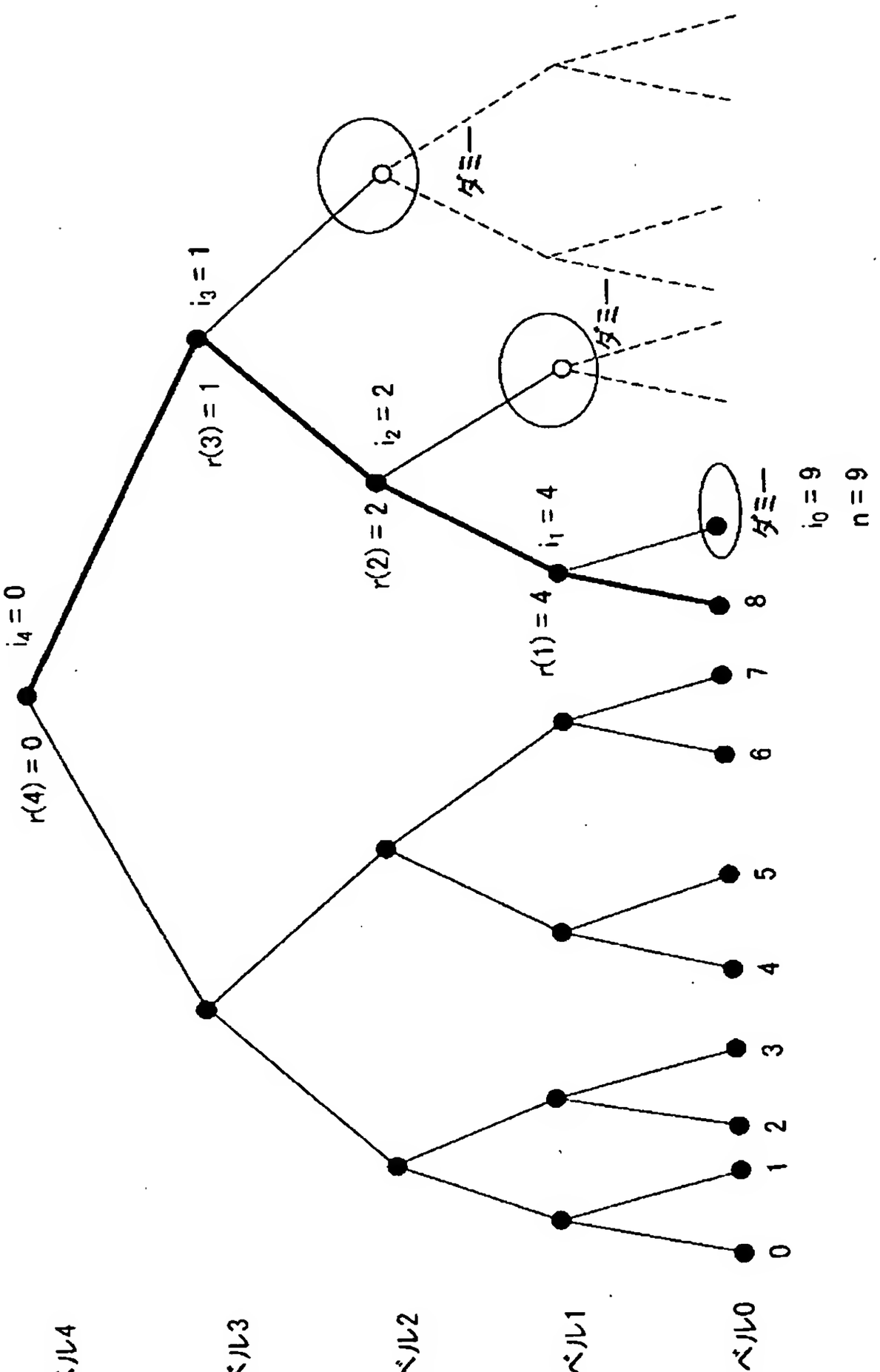
処理手順1

【図２６】

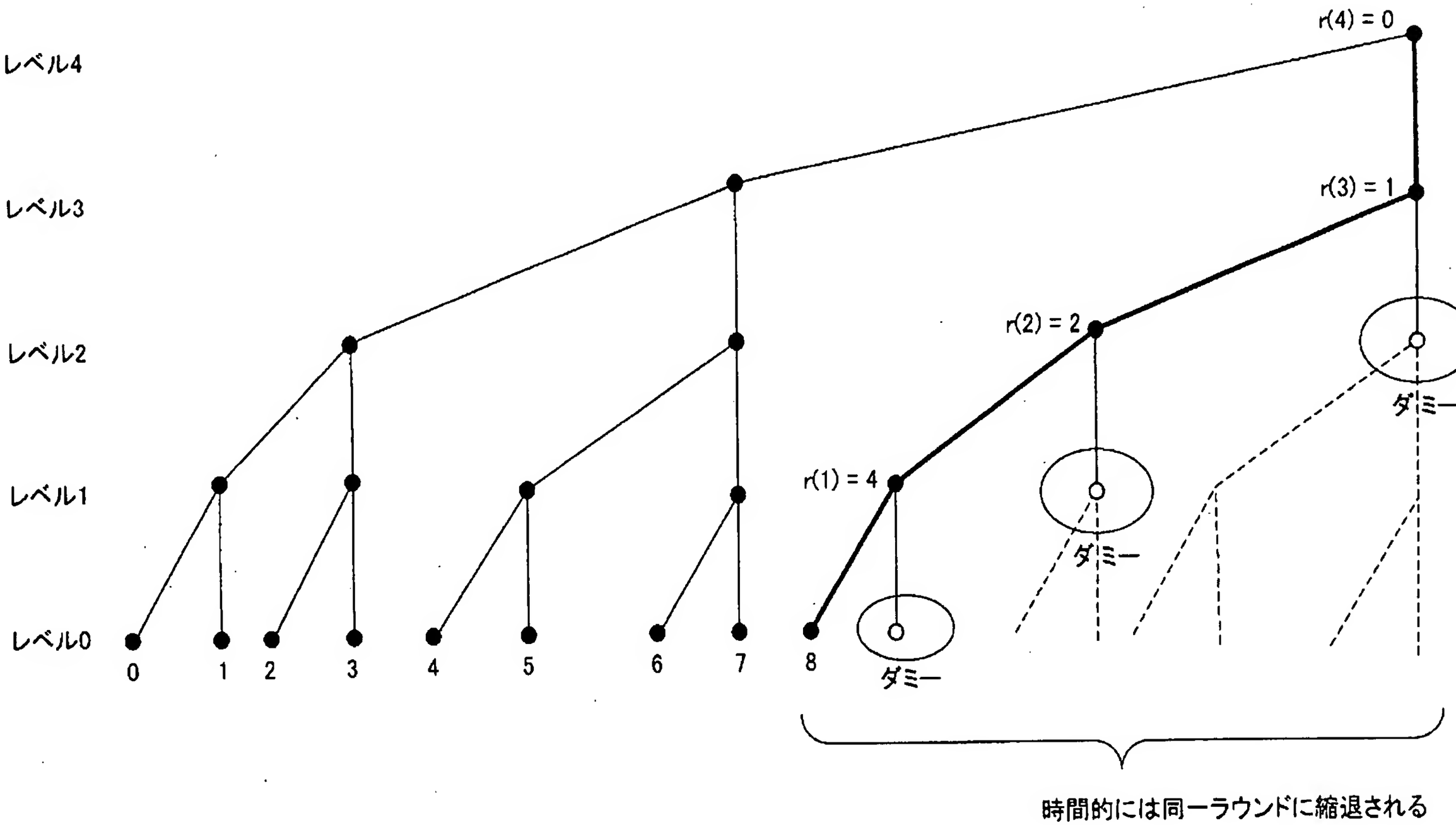
(2)終了時間がきて、ループ1を抜けた後では次の処理を行う.
(2.1) k : = ceiling($\log_2$(n))とおく.
(2.2) rtPath(k,0, n−1) を計算し、その結果を((0, r(0)), ..., (k,r(k)))と置く.
(2.3) ループ3 : j = 0, ..., kに対して以下の処理を行う.
(2.3.1) i = i_j とおく.
(2.3.2) j = 0のとき :
(2.3.2.1) i が奇数のとき :
・ダミー値 r : = R(0,i) を生成する.
・A_j[i] : = r
(ノード (0, i) にrを割り当て).
・b_j : = trueと置く.
・i_j を1インクリメントする.
(2.3.2) 0 <j ≦ kのとき :
(2.3.2.1) i = r(j) のとき :
(即ち、ノード(j, i) が rtPath(k, 0, n−1) 上にあるとき):
(2.3.2.1.1) x0 : = A_{j-1}[index(leftChiild(j, i))]
(ノード(j, i) のleft−childに割り付けられた値をx0と置く).
(2.3.2.1.2) x1 : = A_{j-1}[index(rightChild(j, i))]
(ノード(j, i) のright−childに割り付けられた値をx1と置く).
(2.3.2.1.3) x2 : = h(x0 || x1)を計算する
(2.3.2.1.4) A[i] : = x2
(即ち、ノード(j, i) にx2を割り付ける).
(2.3.2.1.5) iが偶数でj<k のとき :
・ i を1インクリメントする.
・ r : = R(j, i)を計算し、A_j[i] : = r
(即ち、ノード(j, i) にrを割り当る).
・ b_j : = trueと置く.
・ i_j : = i+1と置く.
(2.3.2.2) i = r(j)+1で i が奇数でj<k のとき :
・ r : = R(j, i)を計算し、A_j[i] : = r
(即ち、ノード(j, i) にrを割り当る).
・ b_j : = trueと置く.
・ i_jを1インクリメントする.
ループ3終了.

処理手順2

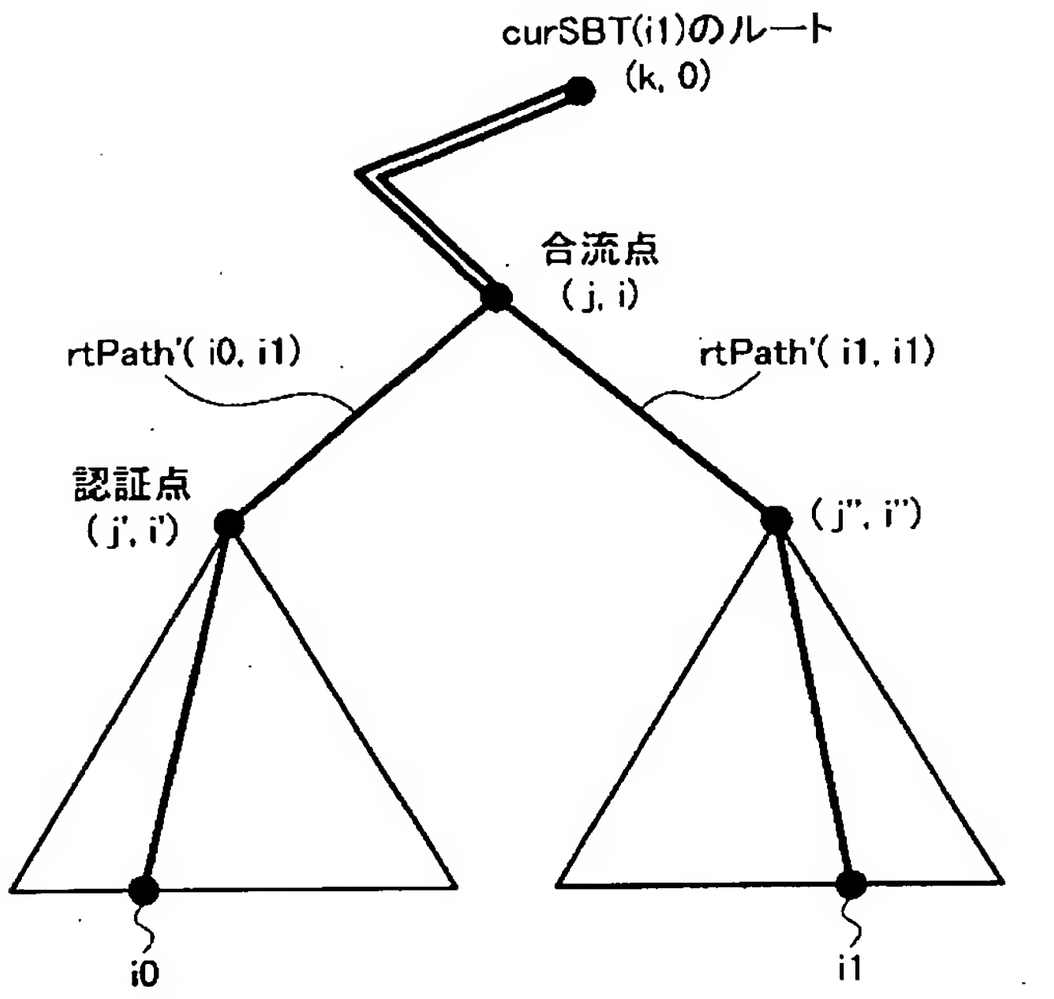
【図２７】


レベル4
レベル3
レベル2
レベル1
レベル0
$i_4 = 0$
$i_3 = 1$
$i_2 = 2$
$i_1 = 4$
$i_0 = 9$
n = 9
r(4) = 0
r(3) = 1
r(2) = 2
r(1) = 4
0
1
2
3
4
5
6
7
8

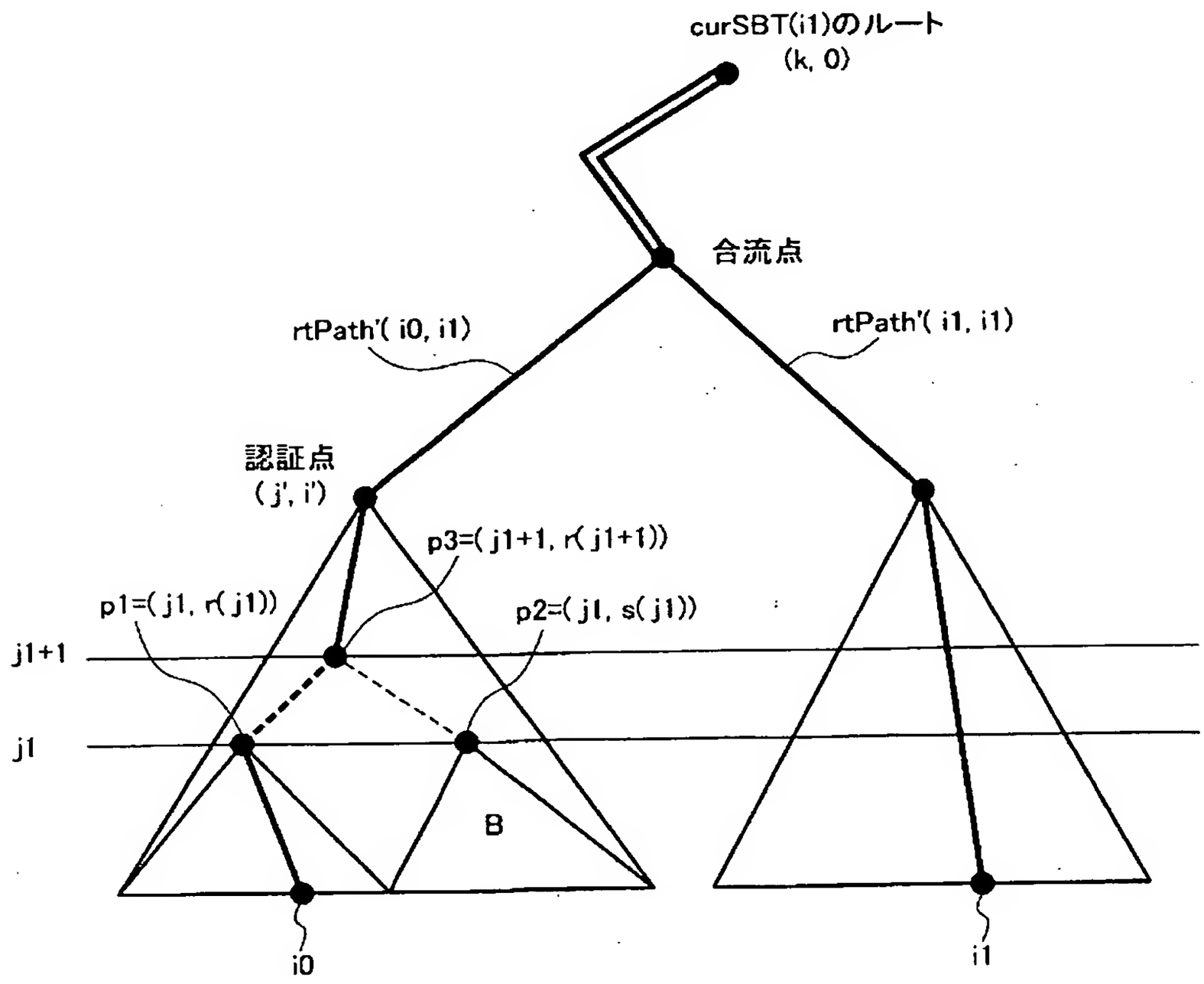
【図２８】


レベル4
レベル3
レベル2
レベル1
レベル0
r(4) = 0
r(3) = 1
r(2) = 2
r(1) = 4
ダミー
ダミー
ダミー
0
1
2
3
4
5
6
7
8
時間的には同一ラウンドに縮退される

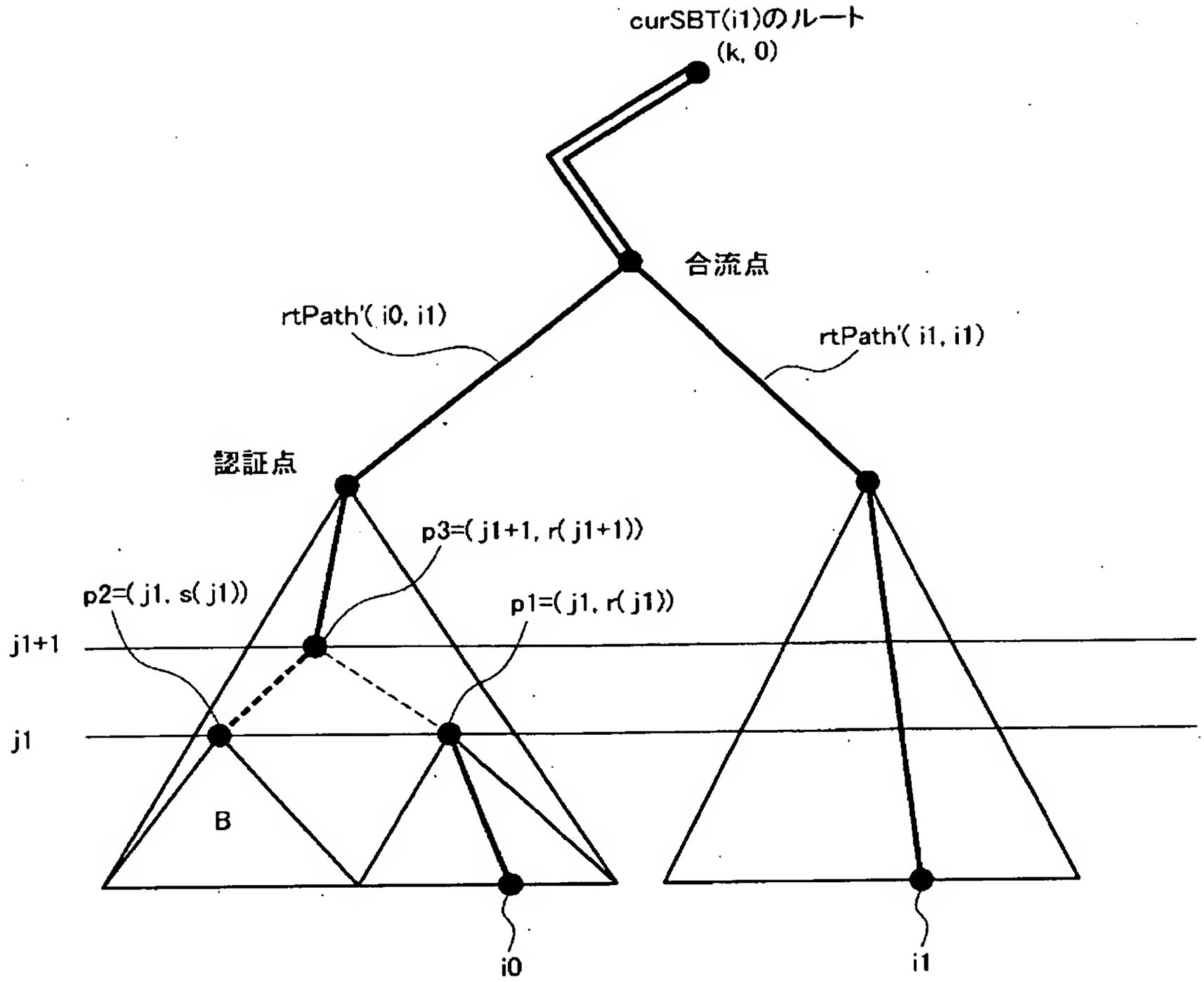
【図２９】


curSBT(i1)のルート
(k, 0)
合流点
(j, i)
rtPath'(i0, i1)
rtPath'(i1, i1)
認証点
(j', i')
(j'', i'')
i0
i1

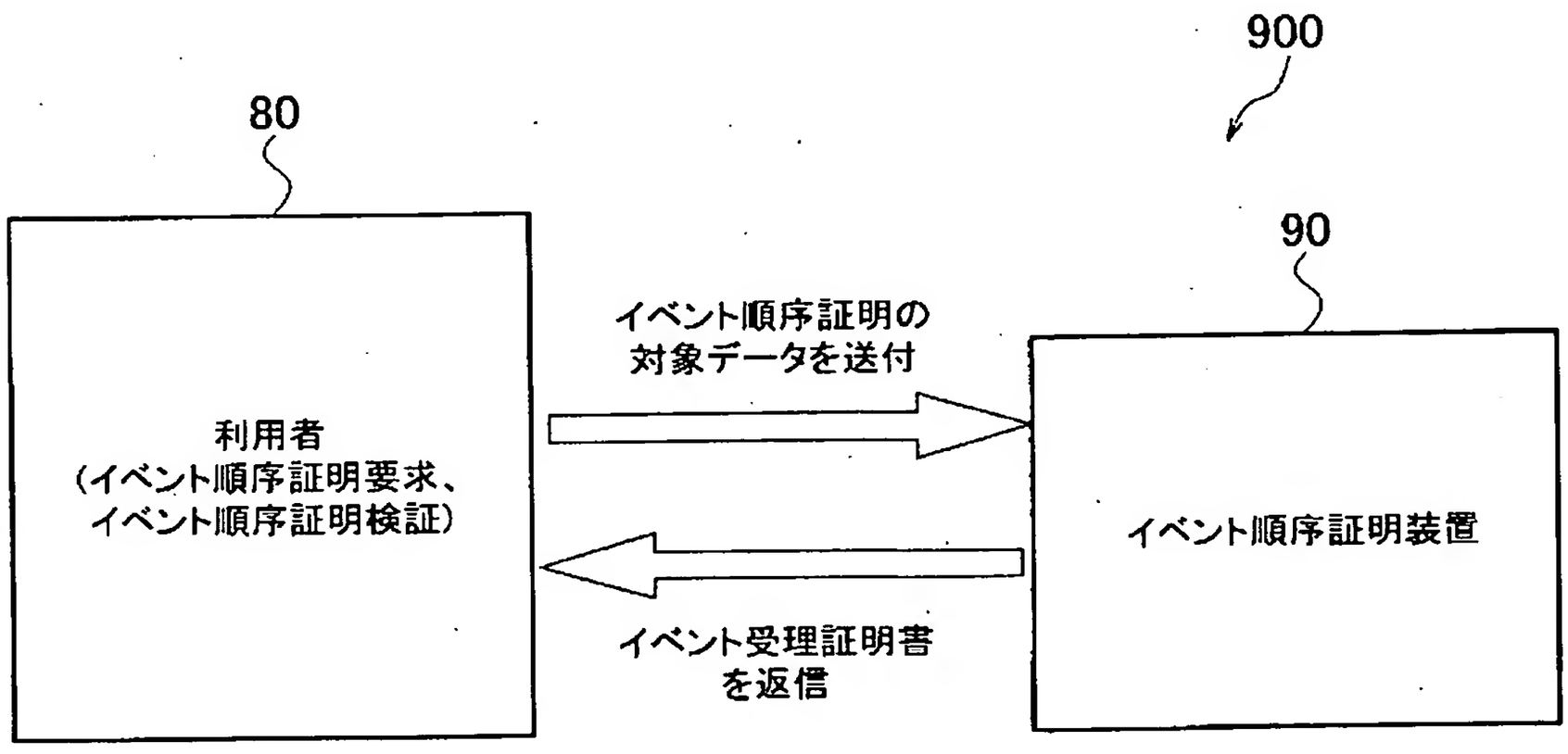
【図３０】


curSBT(i1)のルート
(k, 0)
合流点
rtPath'(i0, i1)
rtPath'(i1, i1)
認証点
(j', i')
p3=(j1+1, r(j1+1))
p1=(j1, r(j1))
p2=(j1, s(j1))
j1+1
j1
B
i0
i1

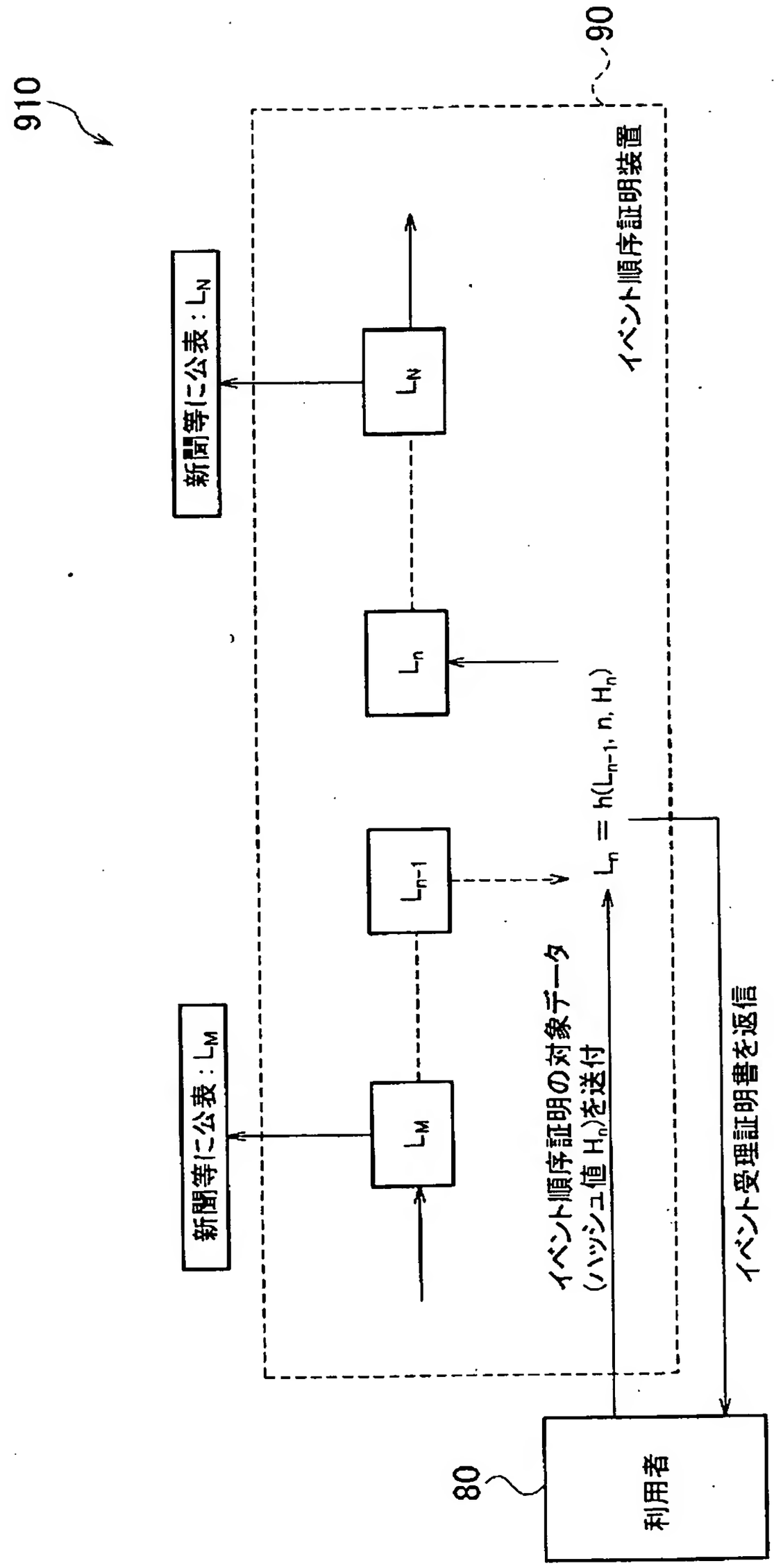
【図３１】


curSBT(i1)のルート
(k, 0)
合流点
rtPath'(i0, i1)
rtPath'(i1, i1)
認証点
p3=(j1+1, r(j1+1))
p2=(j1, s(j1))
p1=(j1, r(j1))
j1+1
j1
B
i0
i1

【図３２】


900
80
90
利用者
(イベント順序証明要求、
イベント順序証明検証)
イベント順序証明の
対象データを送付
イベント受理証明書
を返信
イベント順序証明装置

【図３３】


910
90
イベント順序証明装置
新聞等に公表：L_N
L_N
L_n
L_{n-1}
L_M
新聞等に公表：L_M
イベント順序証明の対象データ
(ハッシュ値 H_n)を送付
$L_n = h(L_{n-1}, n, H_n)$
イベント受理証明書を返信
80
利用者

【書類名】要約書
【要約】
【課題】木構造を用いてイベント順序を証明するイベント順序証明システムにおいて、イベント順序証明要求をまとめた公表データを用いなくても、イベント順序証明機関から発行されたイベント順序受理証明書の検証を行うことができる。
【解決手段】イベント順序証明システム100は、証明装置1、複数の利用者装置2i（i=a，b，…，n）、証明装置1が発行したイベント順序受理証明書の監査を行う監査装置3、及び、以上の各装置を相互に接続するコンピュータネットワーク4を備えており、証明装置1が利用者装置2iからのイベント順序証明要求に応えて、イベント順序受理証明書を発行し、利用者装置2iに返信すると共に、イベント順序受理証明書に疑義が生じた場合には、利用者装置2iは、証明装置1が公表したデータ又は監査装置3による監査結果によってイベント順序受理証明書を検証する。
【選択図】図1

出願人履歴

０００００４２２６
19990715
住所変更
５９１０２９２８６

東京都千代田区大手町二丁目３番１号
日本電信電話株式会社

FIG. 1

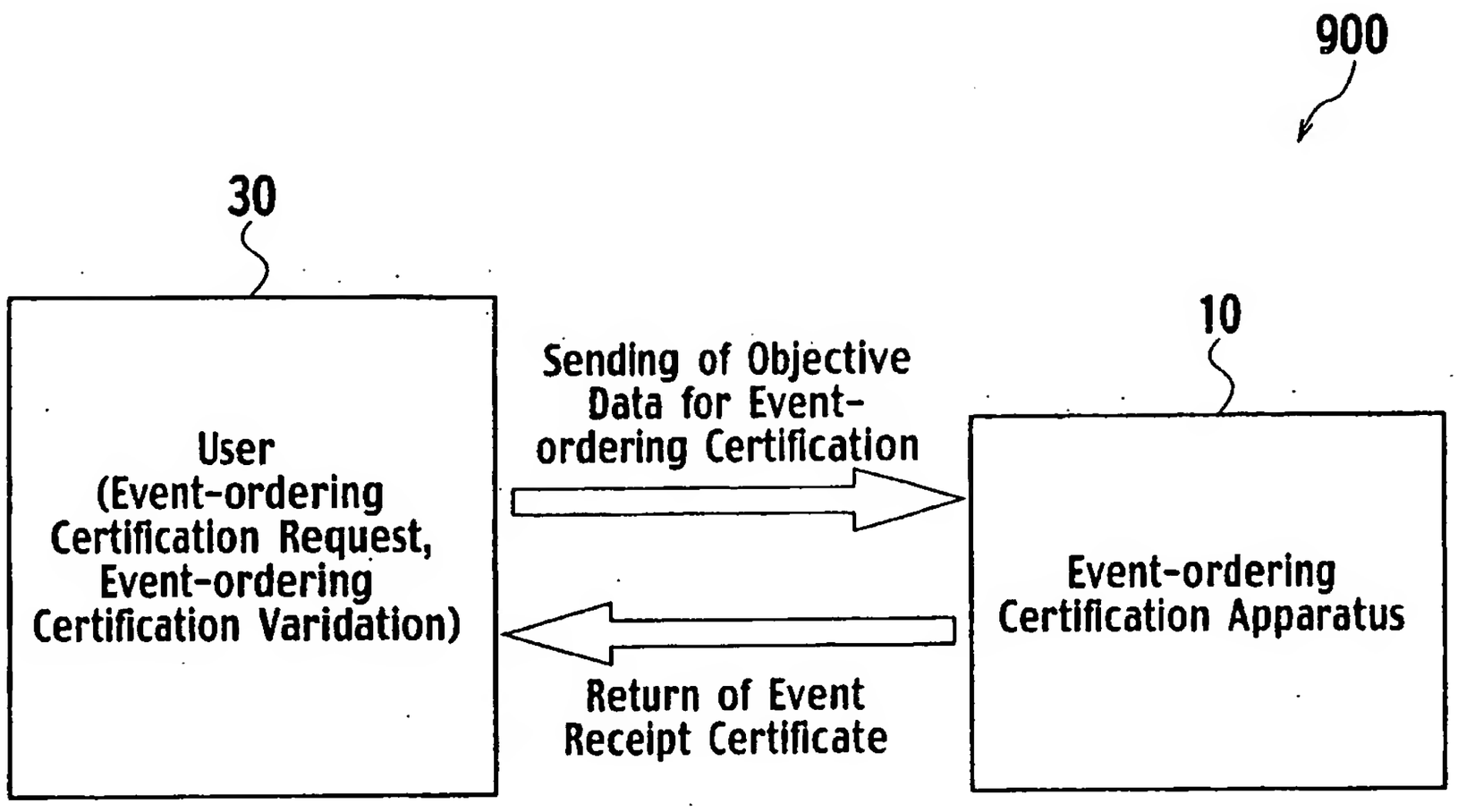

900
30
10
User
(Event-ordering
Certification Request,
Event-ordering
Certification Varidation)
Sending of Objective
Data for Event-
ordering Certification
Return of Event
Receipt Certificate
Event-ordering
Certification Apparatus

FIG. 2

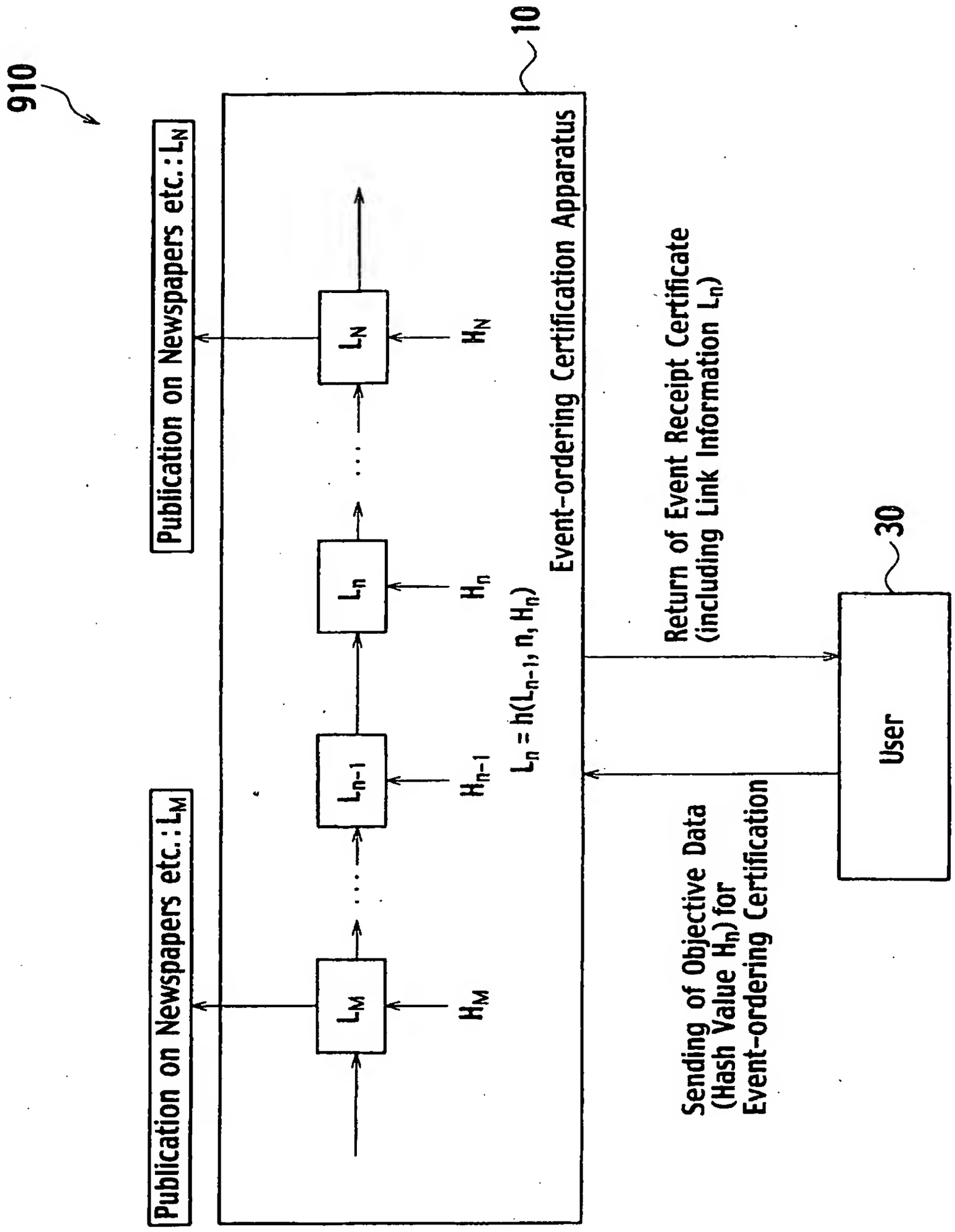

910
10
Publication on Newspapers etc.: L_N
Publication on Newspapers etc.: L_M
L_N
L_n
L_{n-1}
L_M
H_N
H_n
H_{n-1}
H_M
$L_n = h(L_{n-1}, n, H_n)$
Event-ordering Certification Apparatus
Return of Event Receipt Certificate (including Link Information L_n)
Sending of Objective Data (Hash Value H_n) for Event-ordering Certification
30
User

FIG. 3

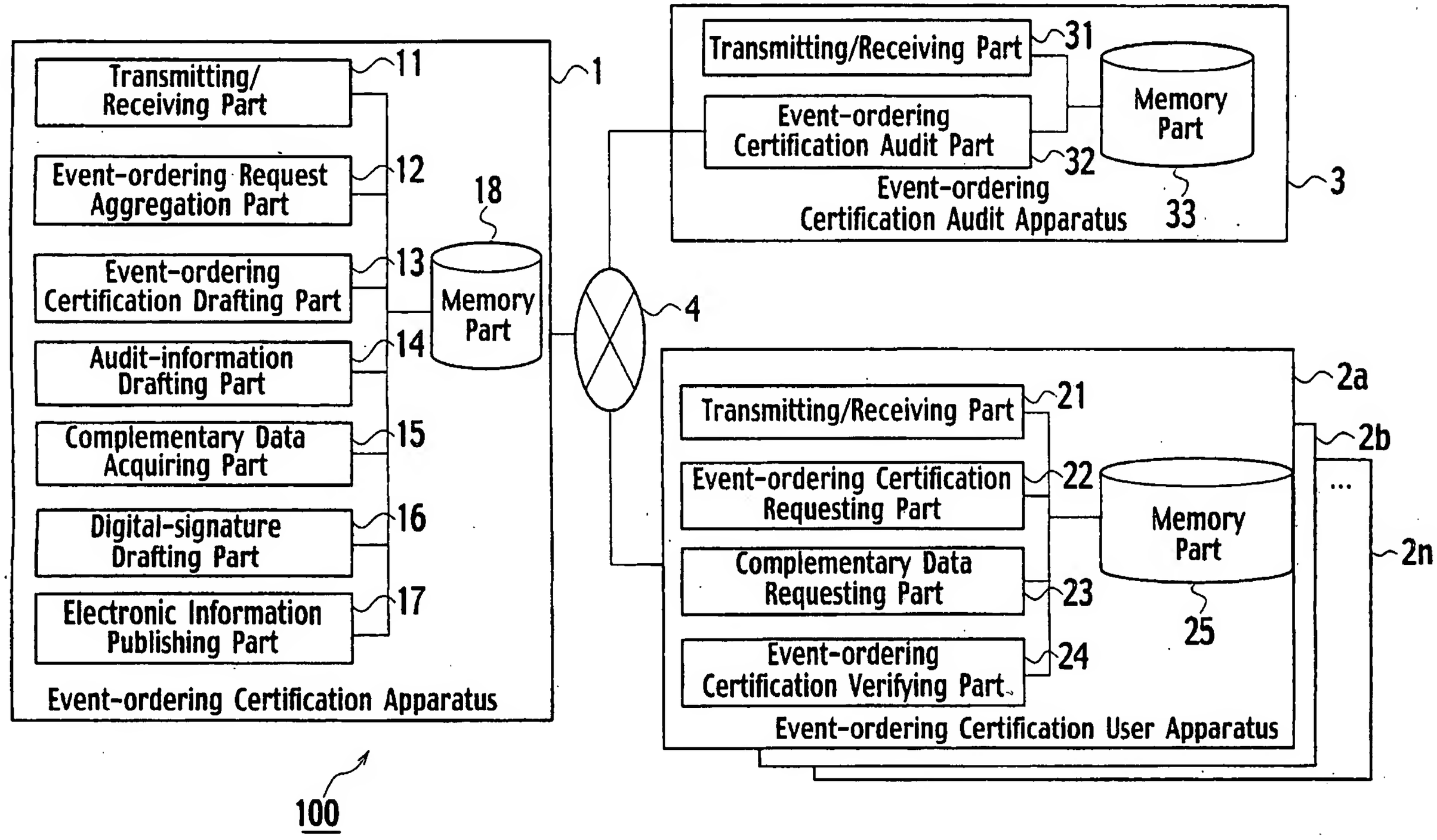

Transmitting/
Receiving Part
11
Event-ordering Request
Aggregation Part
12
Event-ordering
Certification Drafting Part
13
Audit-information
Drafting Part
14
Complementary Data
Acquiring Part
15
Digital-signature
Drafting Part
16
Electronic Information
Publishing Part
17
18
Memory
Part
Event-ordering Certification Apparatus
1
100
4
Transmitting/Receiving Part
31
Event-ordering
Certification Audit Part
32
Memory
Part
33
Event-ordering
Certification Audit Apparatus
3
Transmitting/Receiving Part
21
Event-ordering Certification
Requesting Part
22
Complementary Data
Requesting Part
23
Event-ordering
Certification Verifying Part
24
Memory
Part
25
Event-ordering Certification User Apparatus
2a
2b
...
2n

FIG. 4

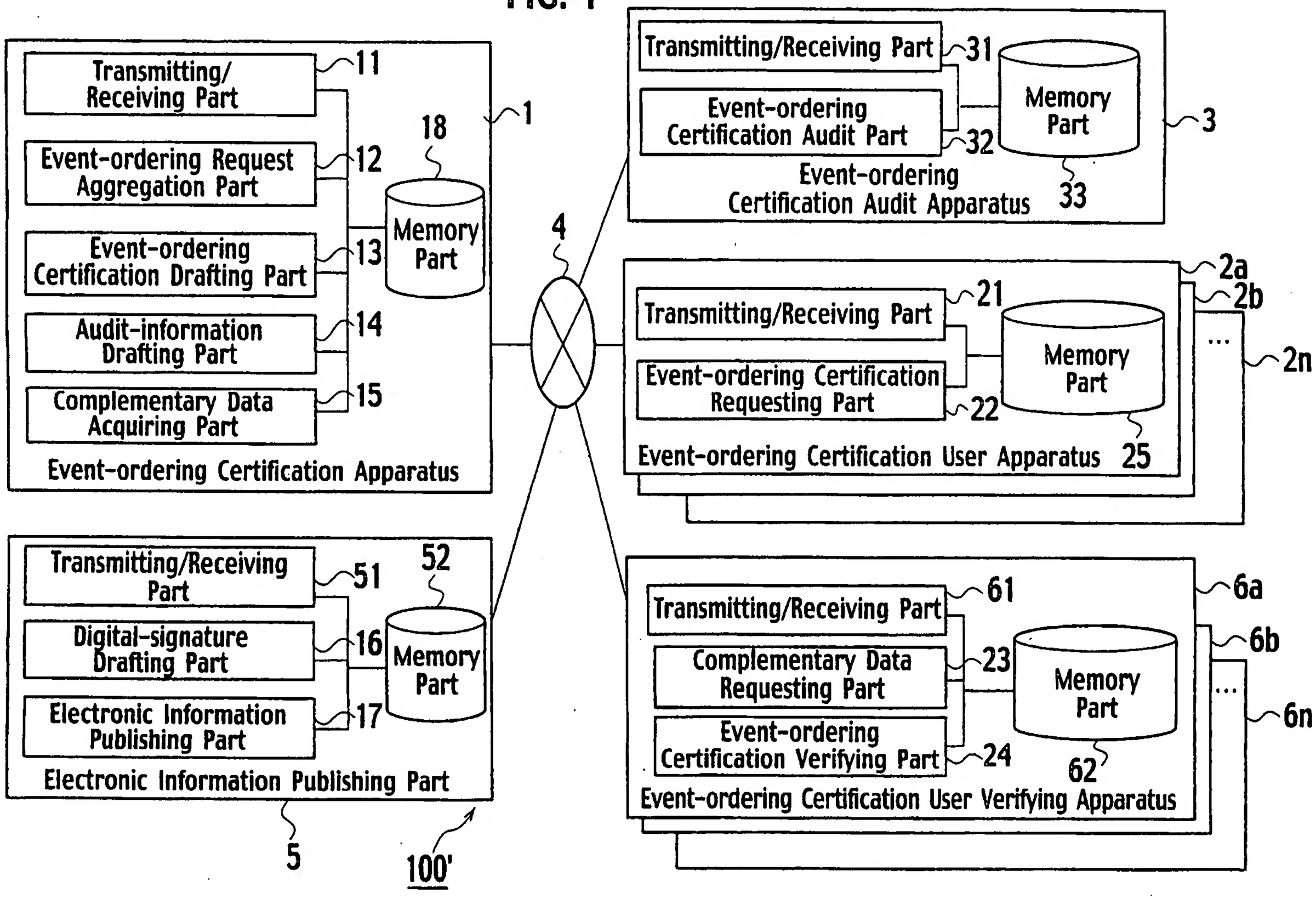

Transmitting/
Receiving Part
11
Event-ordering Request
Aggregation Part
12
Event-ordering
Certification Drafting Part
13
Audit-information
Drafting Part
14
Complementary Data
Acquiring Part
15
18
Memory
Part
1
Event-ordering Certification Apparatus
Transmitting/Receiving Part
31
Event-ordering
Certification Audit Part
32
Memory
Part
3
Event-ordering
Certification Audit Apparatus
33
4
2a
2b
2n
Transmitting/Receiving Part
21
Event-ordering Certification
Requesting Part
22
Memory
Part
Event-ordering Certification User Apparatus
25
Transmitting/Receiving
Part
51
52
Digital-signature
Drafting Part
16
Electronic Information
Publishing Part
17
Memory
Part
Electronic Information Publishing Part
5
100'
6a
6b
6n
Transmitting/Receiving Part
61
Complementary Data
Requesting Part
23
Event-ordering
Certification Verifying Part
24
Memory
Part
62
Event-ordering Certification User Verifying Apparatus

FIG. 5

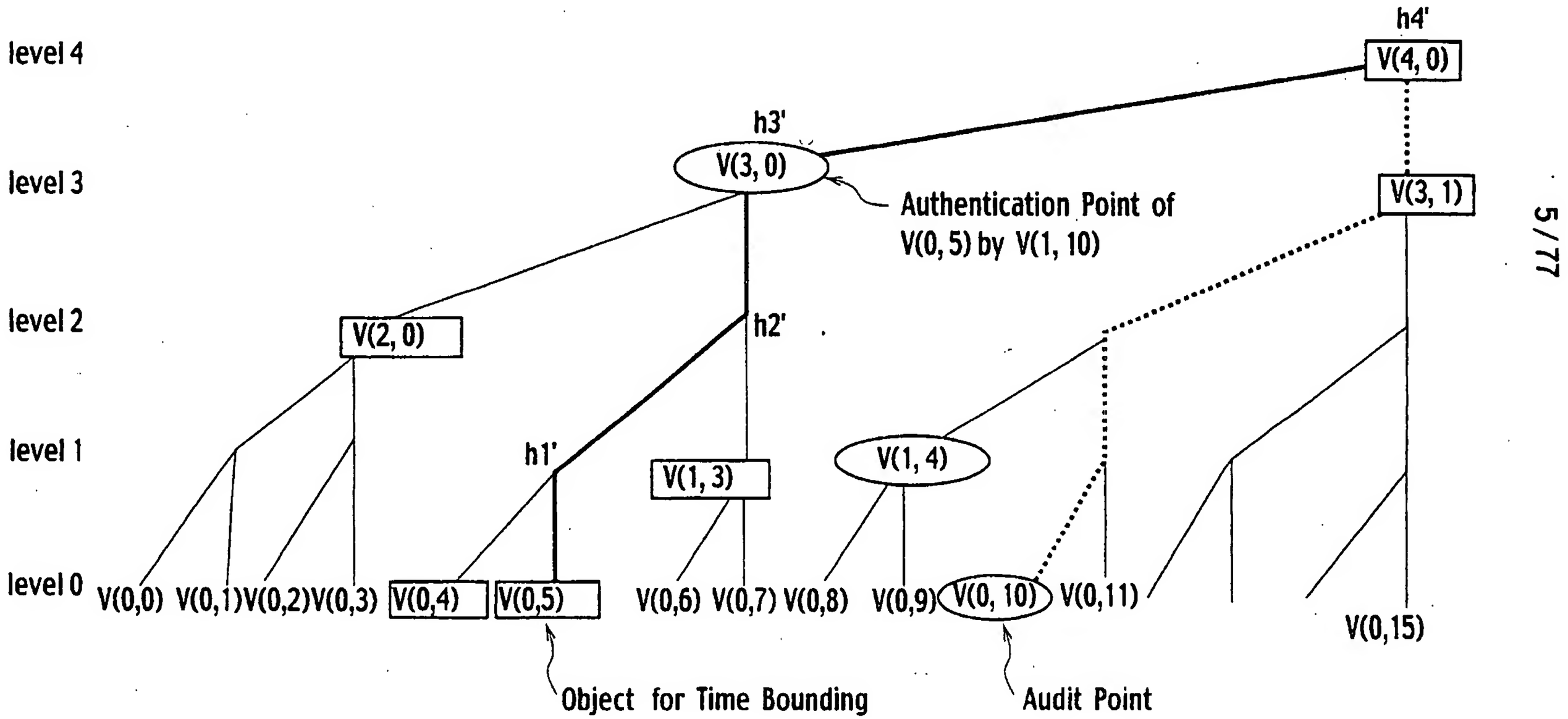

level 4
level 3
level 2
level 1
level 0
h4'
V(4, 0)
h3'
V(3, 0)
Authentication Point of
V(0, 5) by V(1, 10)
V(3, 1)
V(2, 0)
h2'
h1'
V(1, 3)
V(1, 4)
V(0,0) V(0,1) V(0,2) V(0,3)
V(0,4)
V(0,5)
V(0,6) V(0,7) V(0,8)
V(0,9)
V(0, 10)
V(0,11)
V(0,15)
Object for Time Bounding
Audit Point

FIG. 6

ITEM	SIGN	REQUIRED
Original Data	y	○
Sequentially Assigned Data-item	z	○
Sequential Aggregation Tree No.	n	○
Sequential Aggregation Tree Leaf No.	i	○
Immediate Complementary Data (Positional Info. Assigned Value)	HK	
Digital Signature	DS	

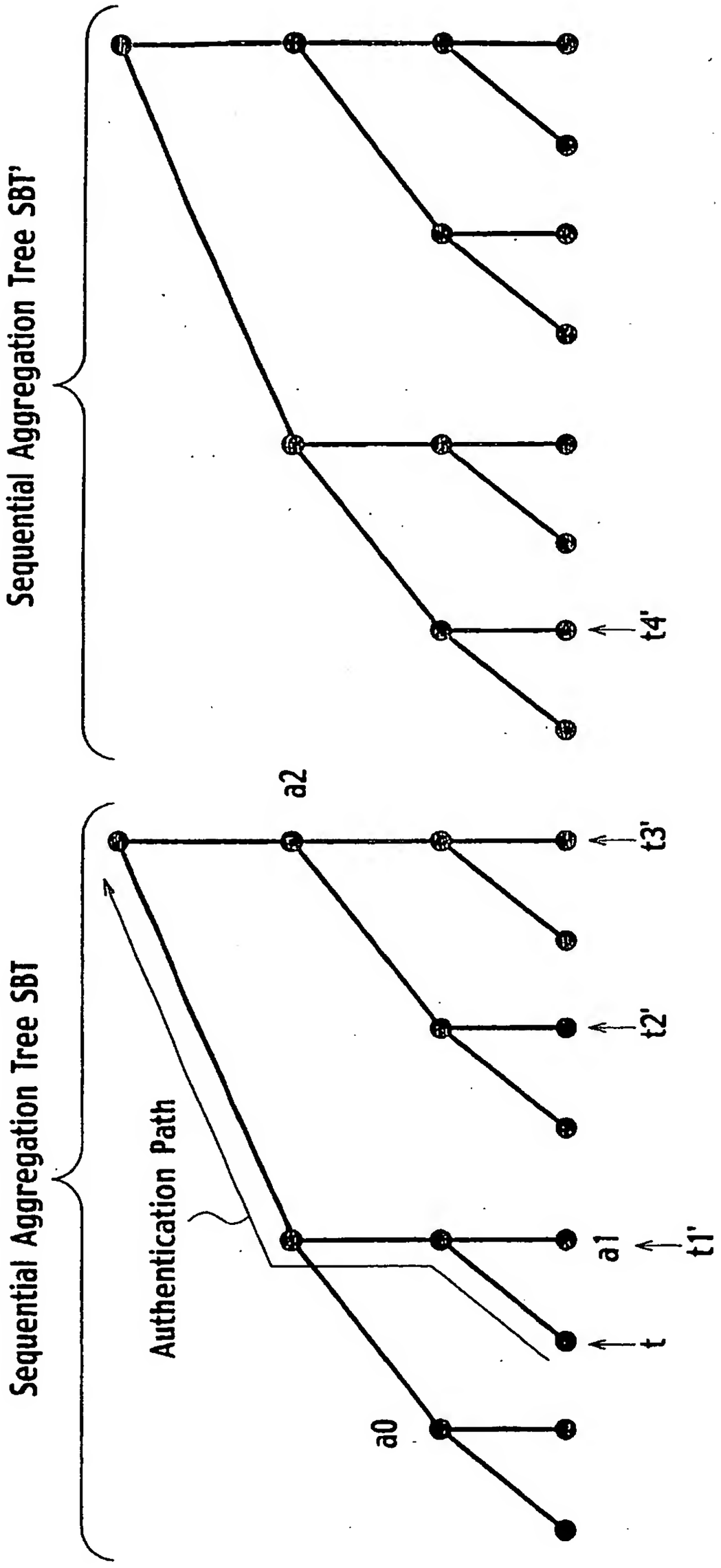

Sequential Aggregation Tree SBT'
Sequential Aggregation Tree SBT
Authentication Path
a2
a1
a0
t4'
t3'
t2'
t1'
t

FIG. 7

FIG. 8

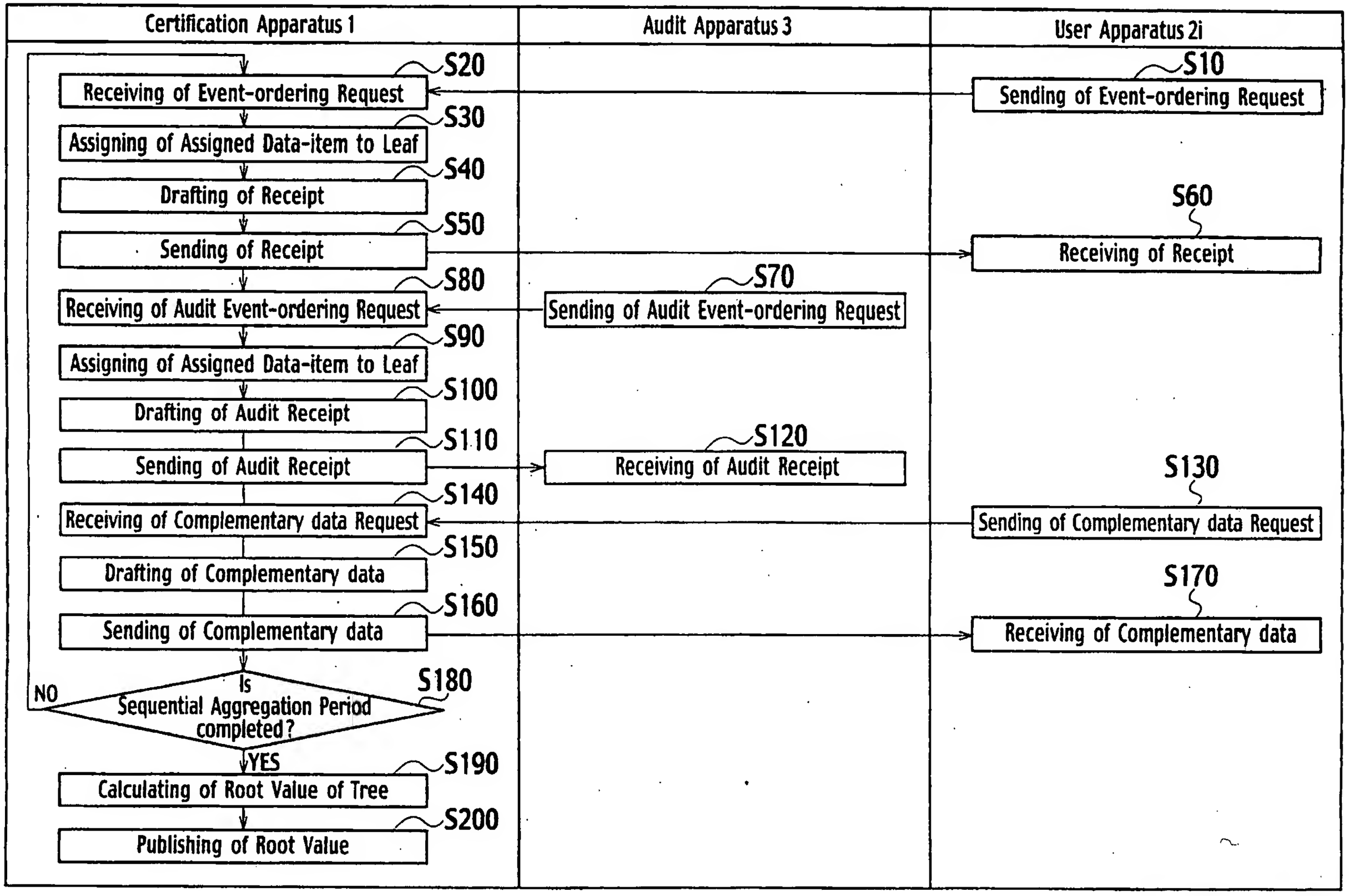

Certification Apparatus 1
Audit Apparatus 3
User Apparatus 2i
S20
Receiving of Event-ordering Request
S10
Sending of Event-ordering Request
S30
Assigning of Assigned Data-item to Leaf
S40
Drafting of Receipt
S60
S50
Sending of Receipt
Receiving of Receipt
S80
S70
Receiving of Audit Event-ordering Request
Sending of Audit Event-ordering Request
S90
Assigning of Assigned Data-item to Leaf
S100
Drafting of Audit Receipt
S110
S120
Sending of Audit Receipt
Receiving of Audit Receipt
S130
S140
Receiving of Complementary data Request
Sending of Complementary data Request
S150
Drafting of Complementary data
S170
S160
Sending of Complementary data
Receiving of Complementary data
NO
Is
Sequential Aggregation Period completed?
S180
YES
S190
Calculating of Root Value of Tree
S200
Publishing of Root Value

FIG. 9

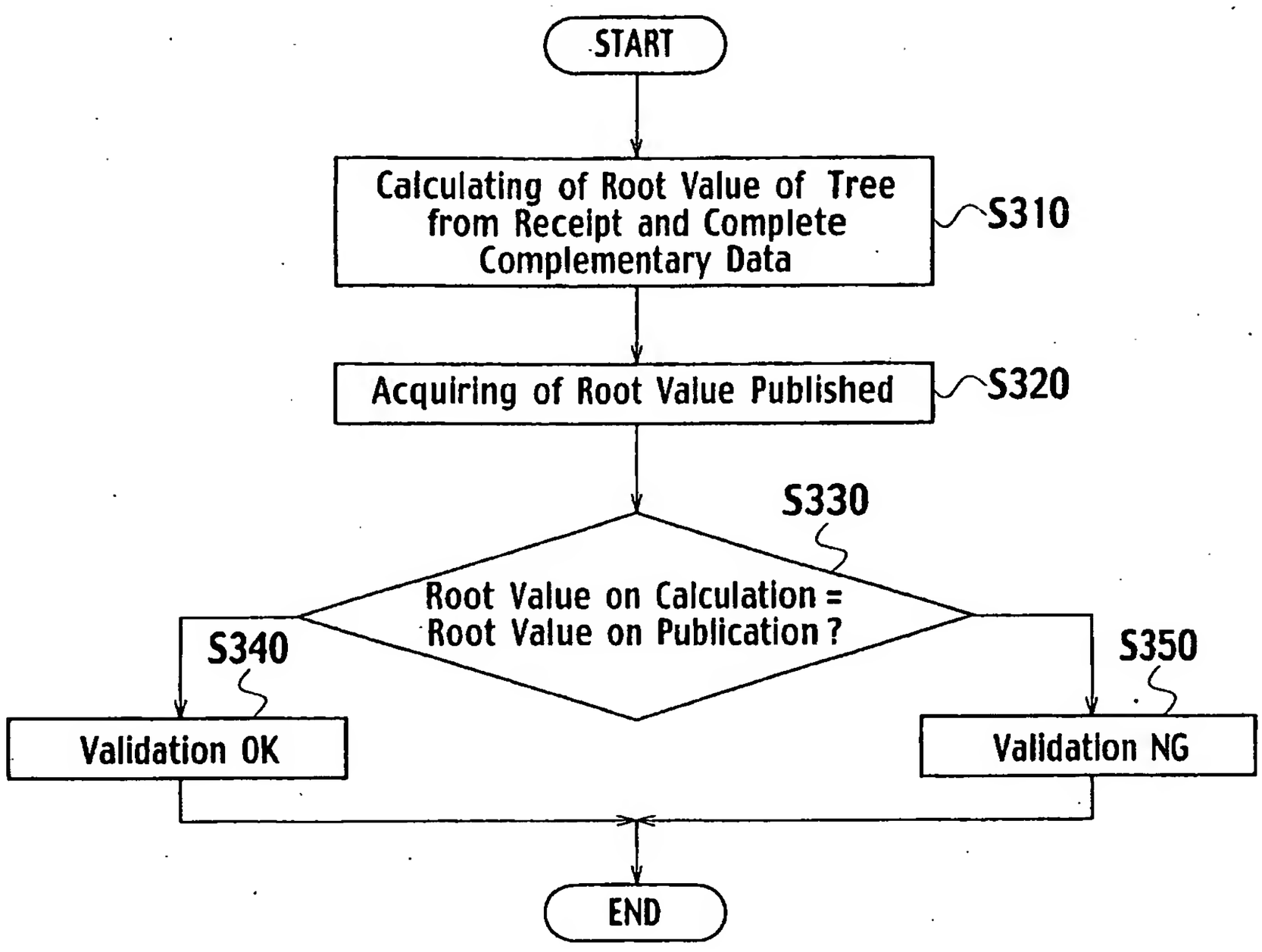

START
Calculating of Root Value of Tree from Receipt and Complete Complementary Data
S310
Acquiring of Root Value Published
S320
S330
Root Value on Calculation = Root Value on Publication ?
S340
Validation OK
S350
Validation NG
END

FIG. 10

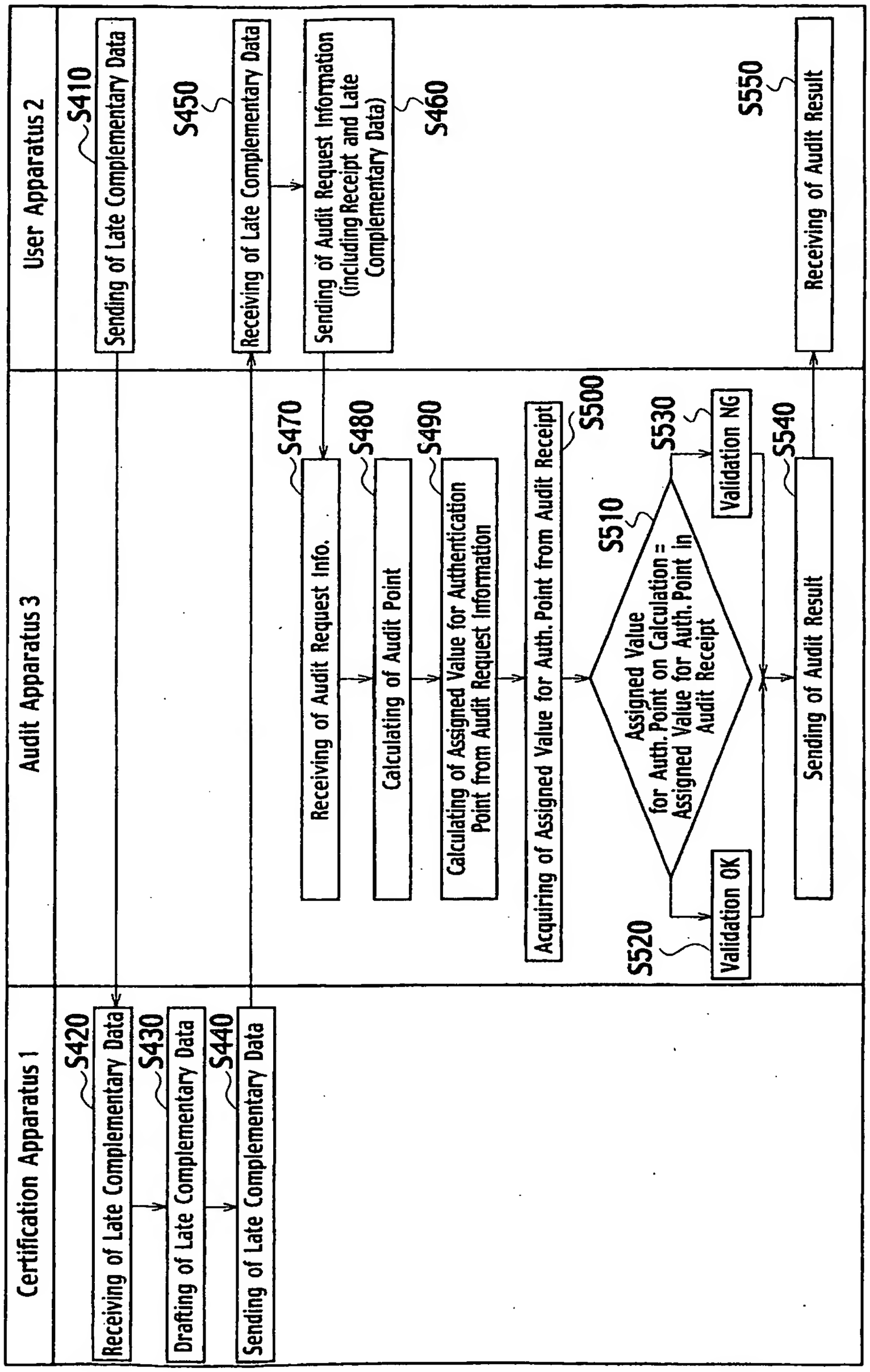

User Apparatus 2
Audit Apparatus 3
Certification Apparatus 1
S410
Sending of Late Complementary Data
S420
Receiving of Late Complementary Data
S430
Drafting of Late Complementary Data
S440
Sending of Late Complementary Data
S450
Receiving of Late Complementary Data
S460
Sending of Audit Request Information (including Receipt and Late Complementary Data)
S470
Receiving of Audit Request Info.
S480
Calculating of Audit Point
S490
Calculating of Assigned Value for Authentication Point from Audit Request Information
S500
Acquiring of Assigned Value for Auth. Point from Audit Receipt
S510
Assigned Value for Auth. Point on Calculation = Assigned Value for Auth. Point in Audit Receipt
S520
Validation OK
S530
Validation NG
S540
Sending of Audit Result
S550
Receiving of Audit Result

FIG. 11

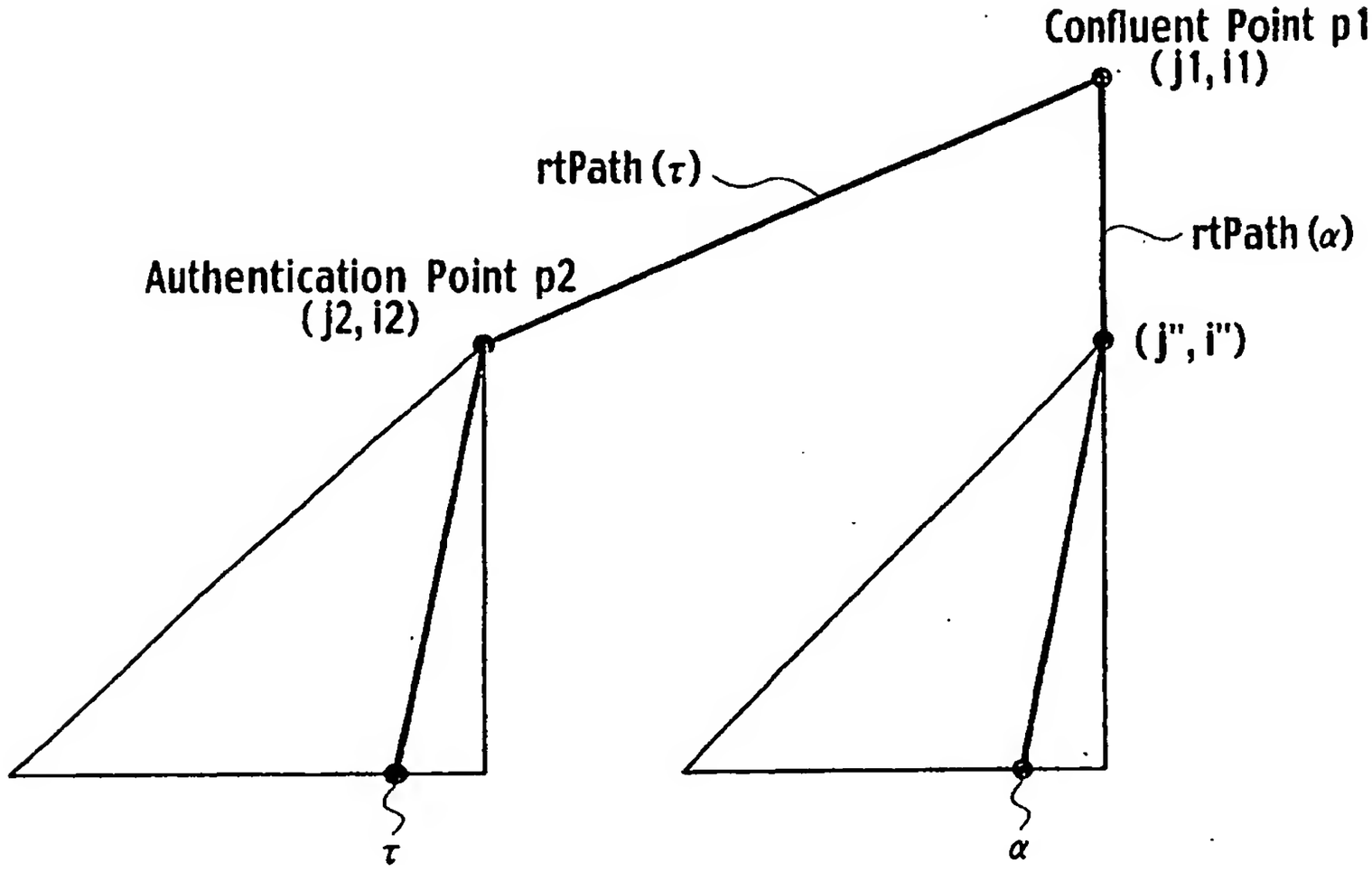

Confluent Point p1
(j1, i1)
rtPath (τ)
rtPath (α)
Authentication Point p2
(j2, i2)
(j", i")
τ
α

FIG. 12

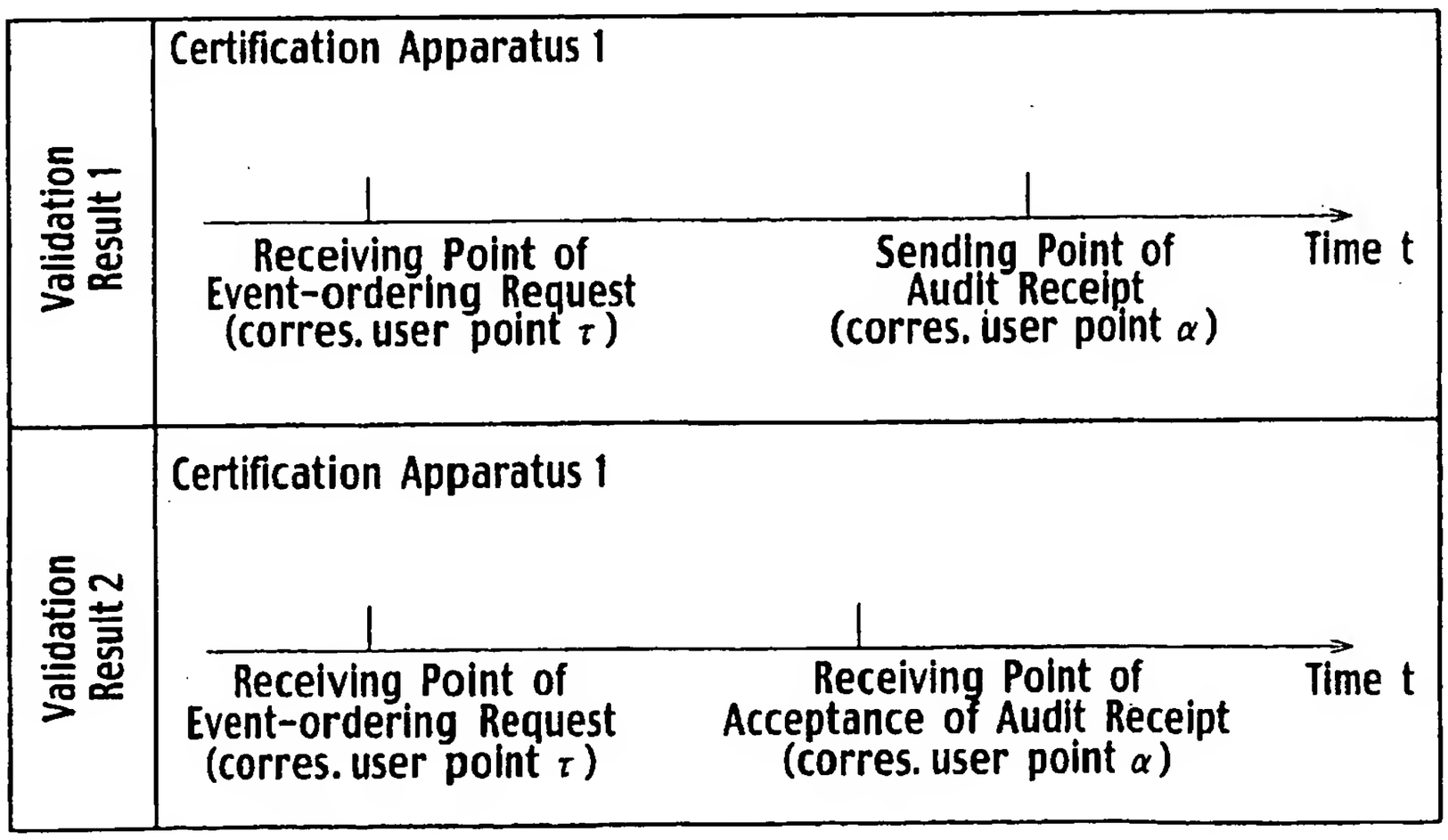

Validation Result 1
Certification Apparatus 1
Receiving Point of Event-ordering Request (corres. user point τ)
Sending Point of Audit Receipt (corres. user point α)
Time t
Validation Result 2
Certification Apparatus 1
Receiving Point of Event-ordering Request (corres. user point τ)
Receiving Point of Acceptance of Audit Receipt (corres. user point α)
Time t

FIG. 13

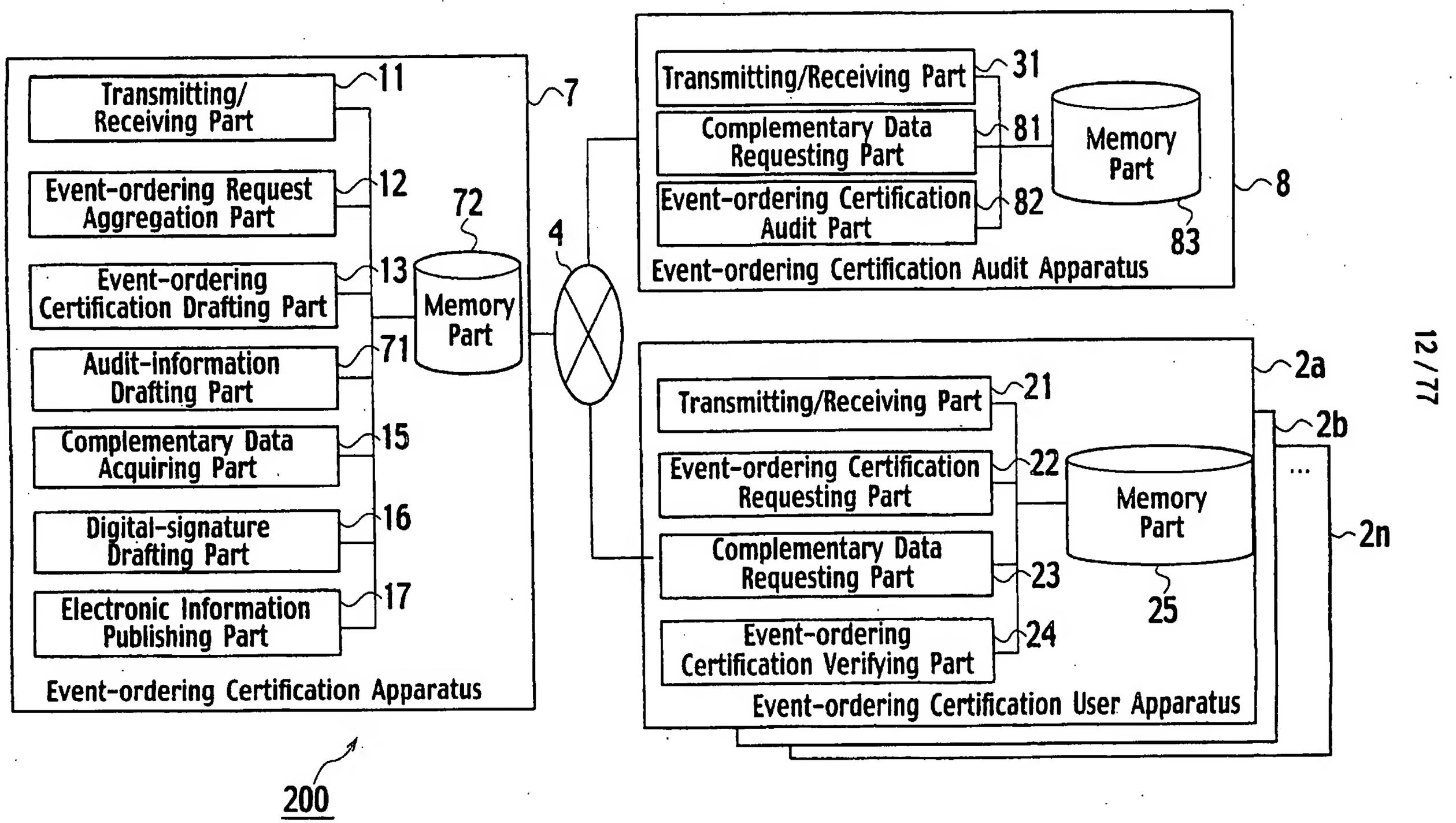

Transmitting/
Receiving Part
11
Event-ordering Request
Aggregation Part
12
Event-ordering
Certification Drafting Part
13
Audit-information
Drafting Part
71
Complementary Data
Acquiring Part
15
Digital-signature
Drafting Part
16
Electronic Information
Publishing Part
17
72
Memory
Part
7
Event-ordering Certification Apparatus
4
Transmitting/Receiving Part
31
Complementary Data
Requesting Part
81
Event-ordering Certification
Audit Part
82
Memory
Part
83
8
Event-ordering Certification Audit Apparatus
Transmitting/Receiving Part
21
Event-ordering Certification
Requesting Part
22
Complementary Data
Requesting Part
23
Event-ordering
Certification Verifying Part
24
Memory
Part
25
2a
2b
...
2n
Event-ordering Certification User Apparatus
200

FIG. 14

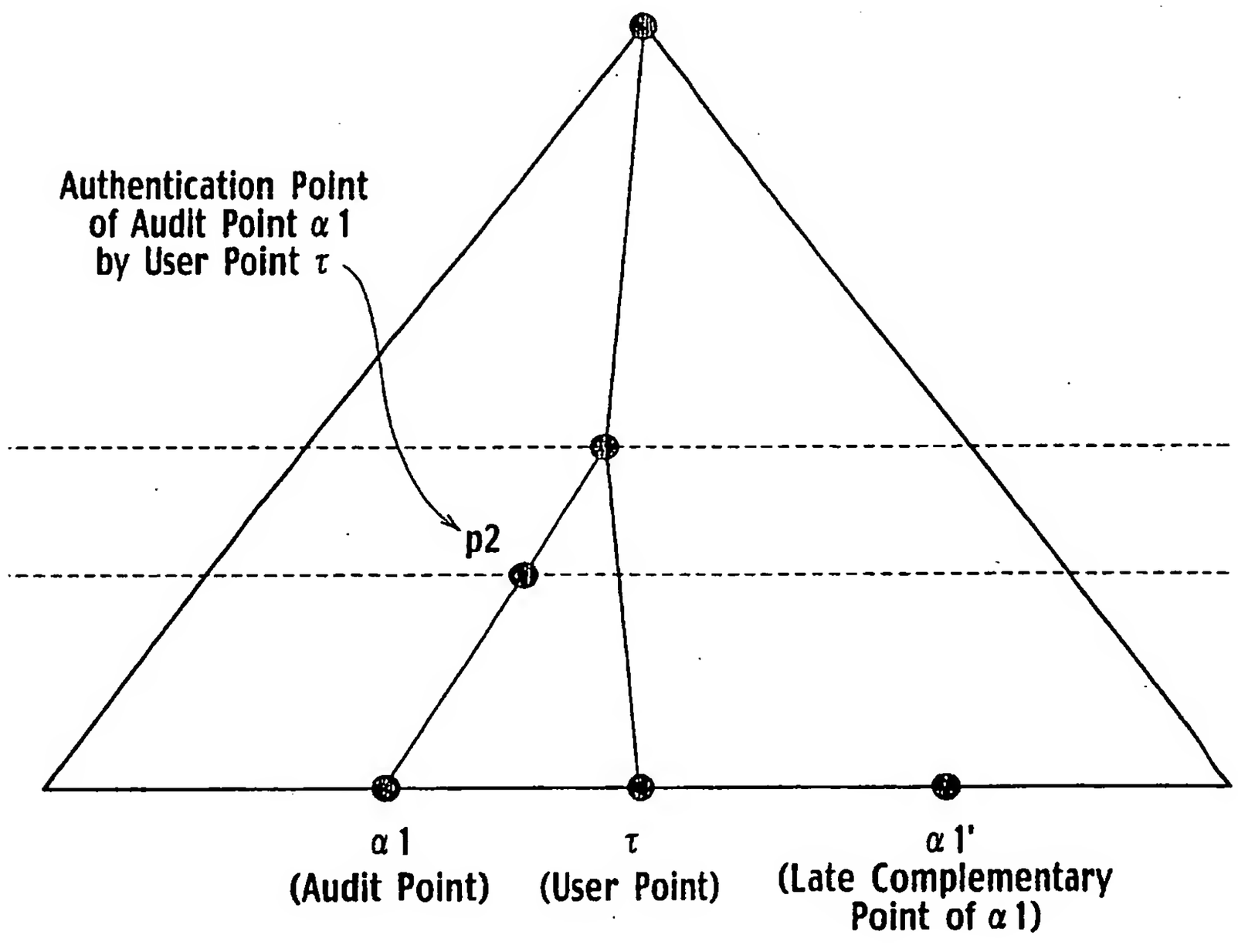

Authentication Point
of Audit Point α 1
by User Point τ
p2
α 1
(Audit Point)
τ
(User Point)
α 1'
(Late Complementary
Point of α 1)

FIG. 15

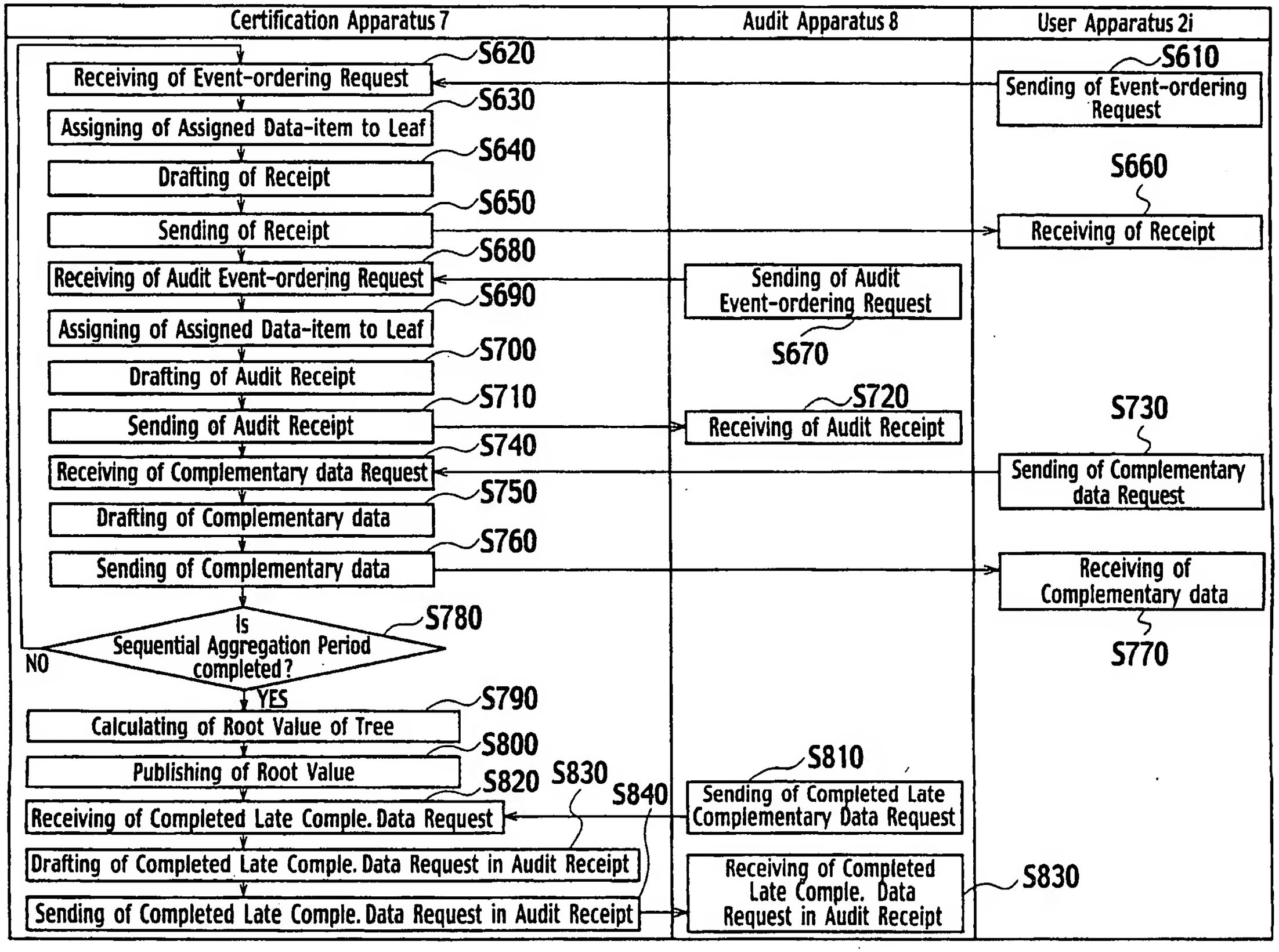

Certification Apparatus 7
Audit Apparatus 8
User Apparatus 2i
S620
Receiving of Event-ordering Request
S610
Sending of Event-ordering Request
S630
Assigning of Assigned Data-item to Leaf
S640
Drafting of Receipt
S660
S650
Sending of Receipt
Receiving of Receipt
S680
Receiving of Audit Event-ordering Request
Sending of Audit Event-ordering Request
S690
Assigning of Assigned Data-item to Leaf
S670
S700
Drafting of Audit Receipt
S710
S720
S730
Sending of Audit Receipt
Receiving of Audit Receipt
S740
Receiving of Complementary data Request
Sending of Complementary data Request
S750
Drafting of Complementary data
S760
Sending of Complementary data
Receiving of Complementary data
S770
S780
Is Sequential Aggregation Period completed?
NO
YES
S790
Calculating of Root Value of Tree
S800
Publishing of Root Value
S810
S820
S830
S840
Receiving of Completed Late Comple. Data Request
Sending of Completed Late Complementary Data Request
Drafting of Completed Late Comple. Data Request in Audit Receipt
Receiving of Completed Late Comple. Data Request in Audit Receipt
S830
Sending of Completed Late Comple. Data Request in Audit Receipt

FIG. 16

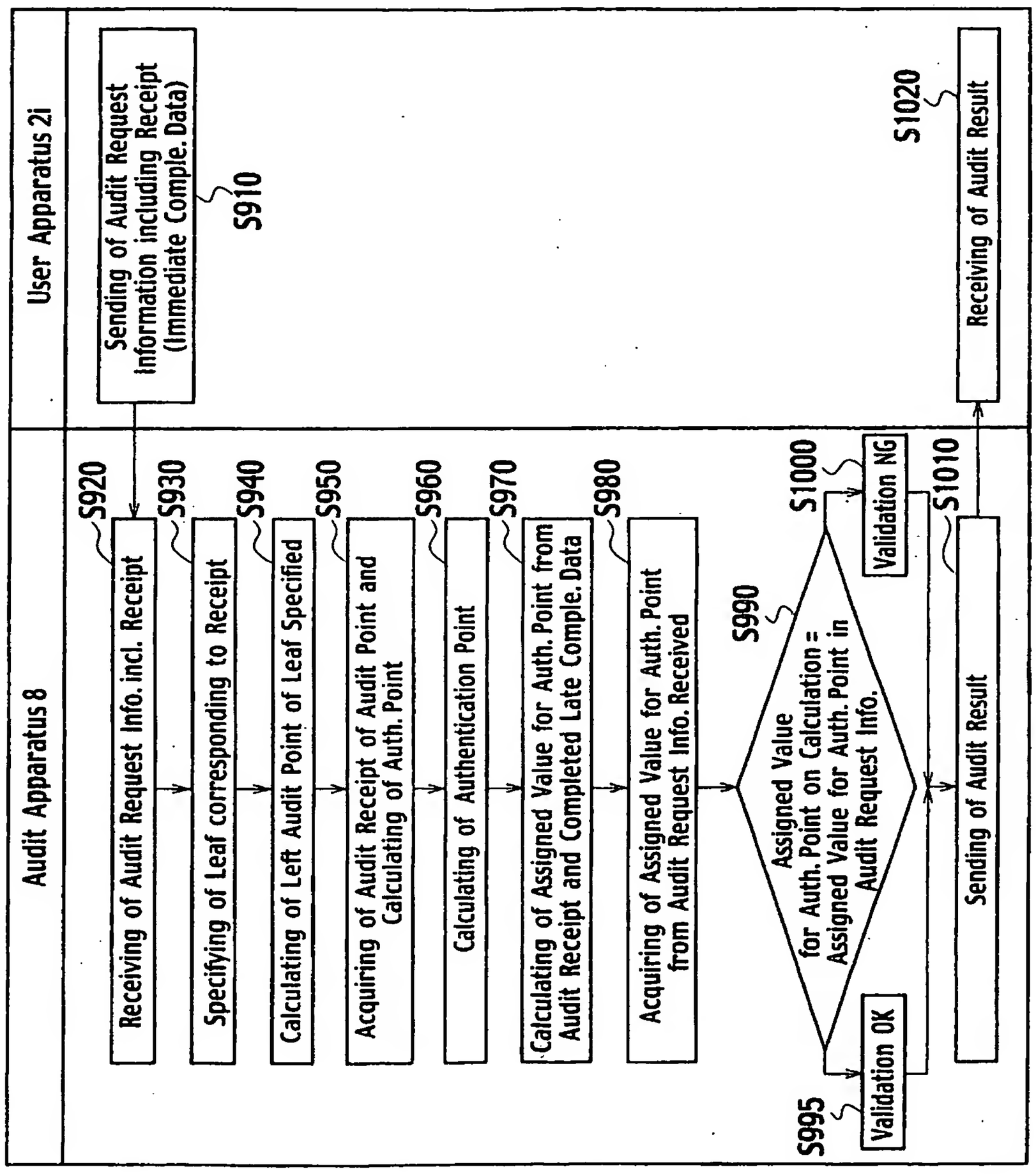

Audit Apparatus 8
User Apparatus 2i
Receiving of Audit Request Info. incl. Receipt
Specifying of Leaf corresponding to Receipt
Calculating of Left Audit Point of Leaf Specified
Acquiring of Audit Receipt of Audit Point and Calculating of Auth. Point
Calculating of Authentication Point
Calculating of Assigned Value for Auth. Point from Audit Receipt and Completed Late Comple. Data
Acquiring of Assigned Value for Auth. Point from Audit Request Info. Received
Assigned Value for Auth. Point on Calculation = Assigned Value for Auth. Point in Audit Request Info.
Validation OK
Validation NG
Sending of Audit Result
Receiving of Audit Result
Sending of Audit Request Information including Receipt (Immediate Comple. Data)
S910
S920
S930
S940
S950
S960
S970
S980
S990
S995
S1000
S1010
S1020

FIG. 17

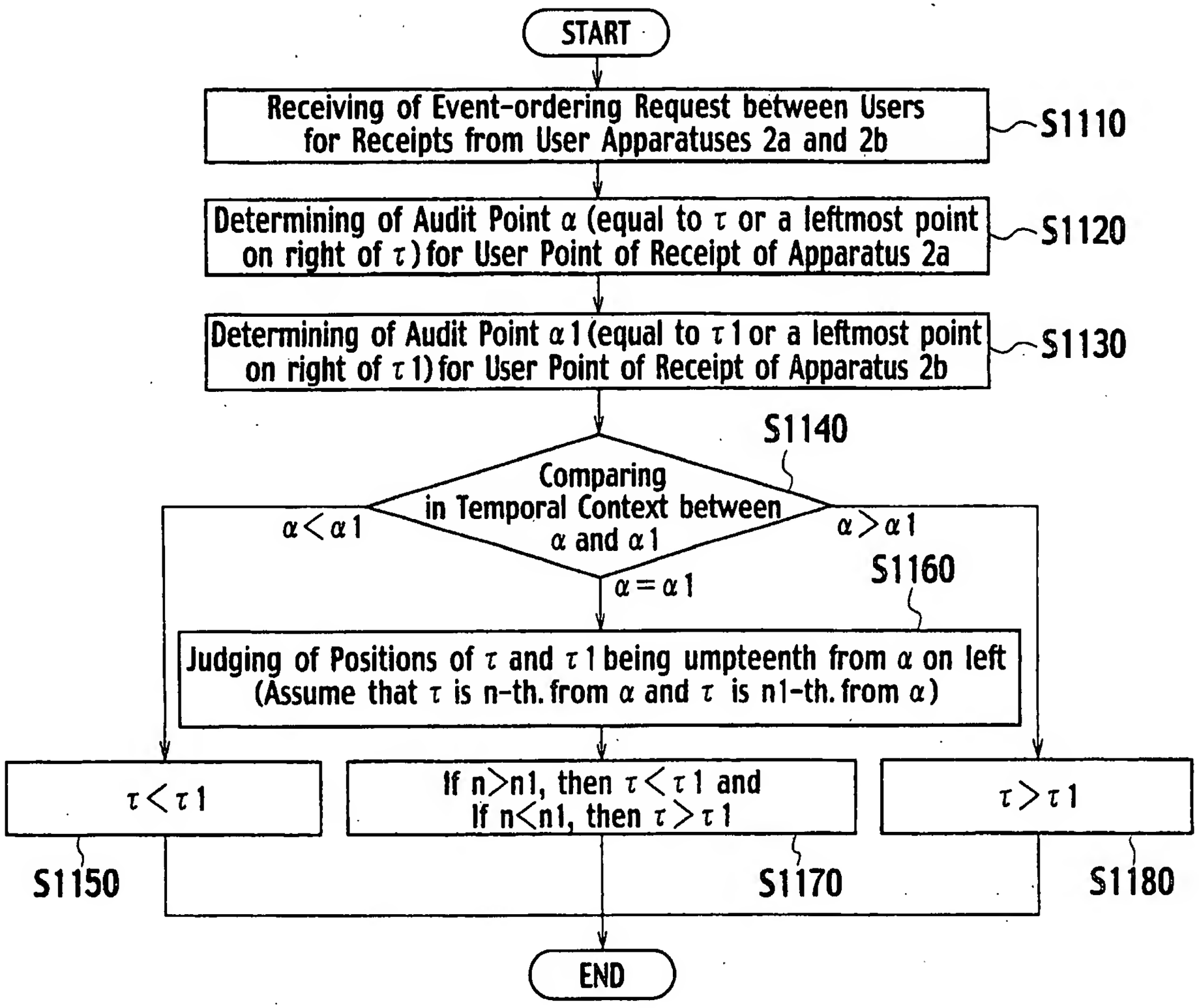

START
Receiving of Event-ordering Request between Users for Receipts from User Apparatuses 2a and 2b
S1110
Determining of Audit Point α (equal to τ or a leftmost point on right of τ) for User Point of Receipt of Apparatus 2a
S1120
Determining of Audit Point α1 (equal to τ1 or a leftmost point on right of τ1) for User Point of Receipt of Apparatus 2b
S1130
S1140
Comparing in Temporal Context between α and α1
α<α1
α>α1
α=α1
S1160
Judging of Positions of τ and τ1 being umpteenth from α on left (Assume that τ is n-th. from α and τ is n1-th. from α)
τ<τ1
If n>n1, then τ<τ1 and If n<n1, then τ>τ1
τ>τ1
S1150
S1170
S1180
END

FIG. 18

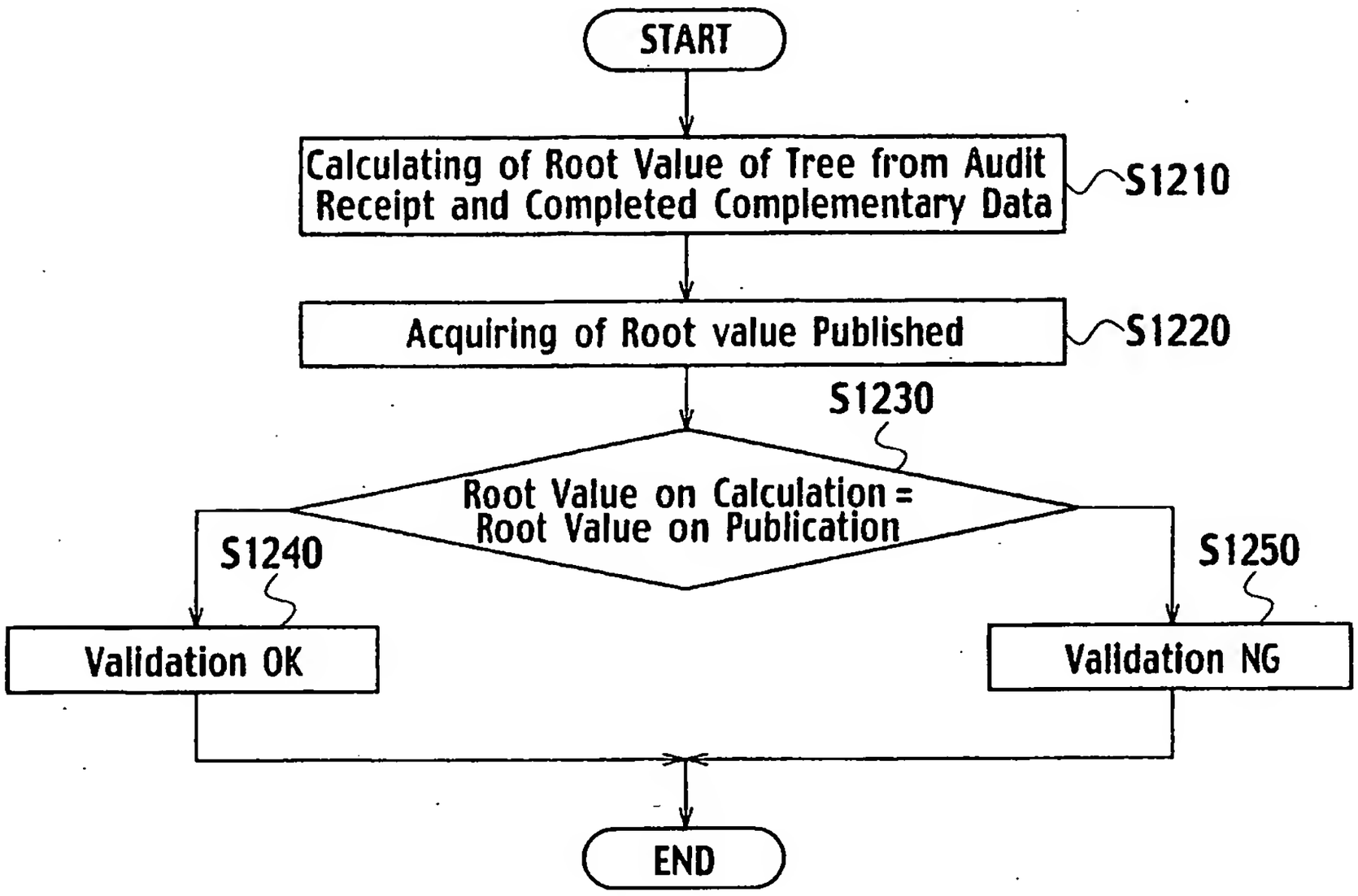

START
Calculating of Root Value of Tree from Audit Receipt and Completed Complementary Data
S1210
Acquiring of Root value Published
S1220
S1230
Root Value on Calculation = Root Value on Publication
S1240
S1250
Validation OK
Validation NG
END

FIG. 19

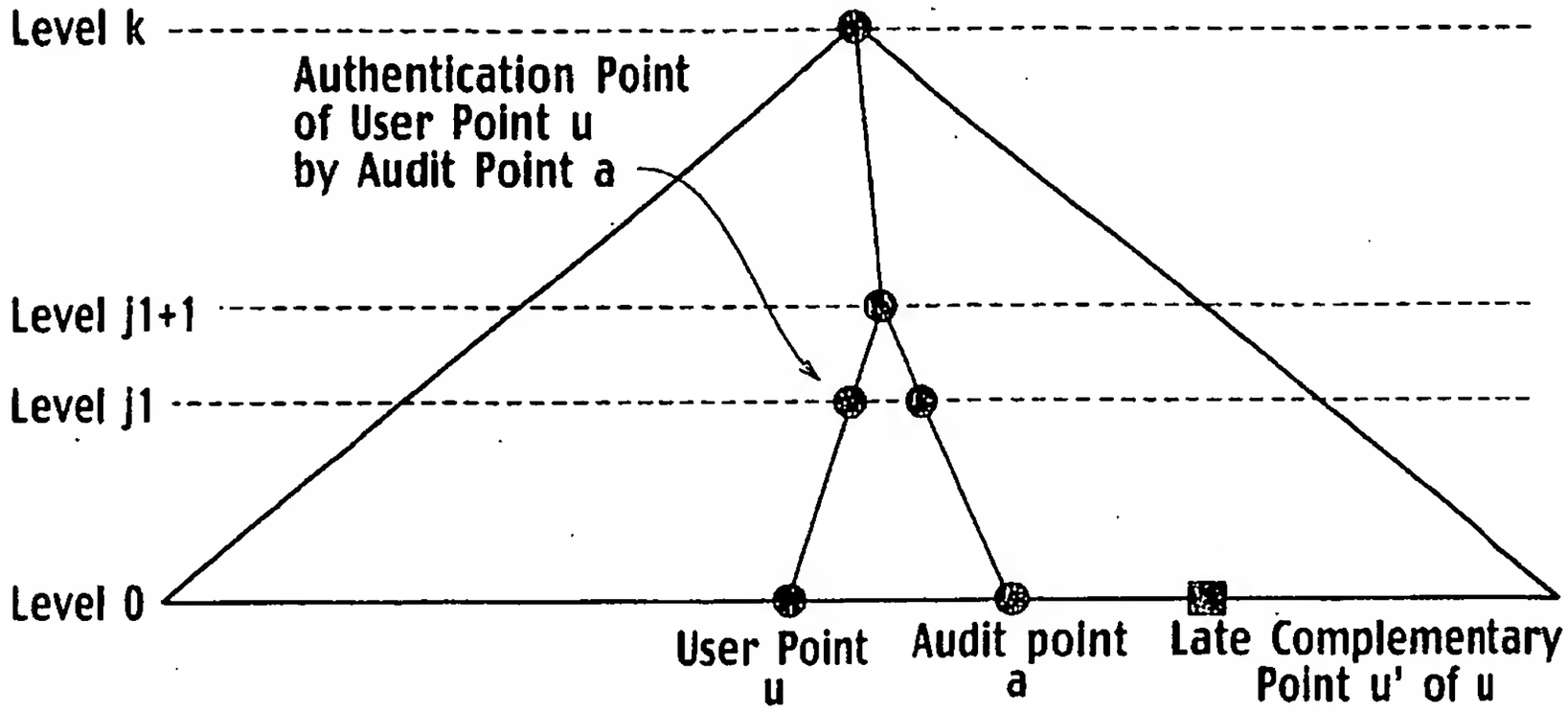

Level k
Authentication Point
of User Point u
by Audit Point a
Level j1+1
Level j1
Level 0
User Point
u
Audit point
a
Late Complementary
Point u' of u

FIG. 20

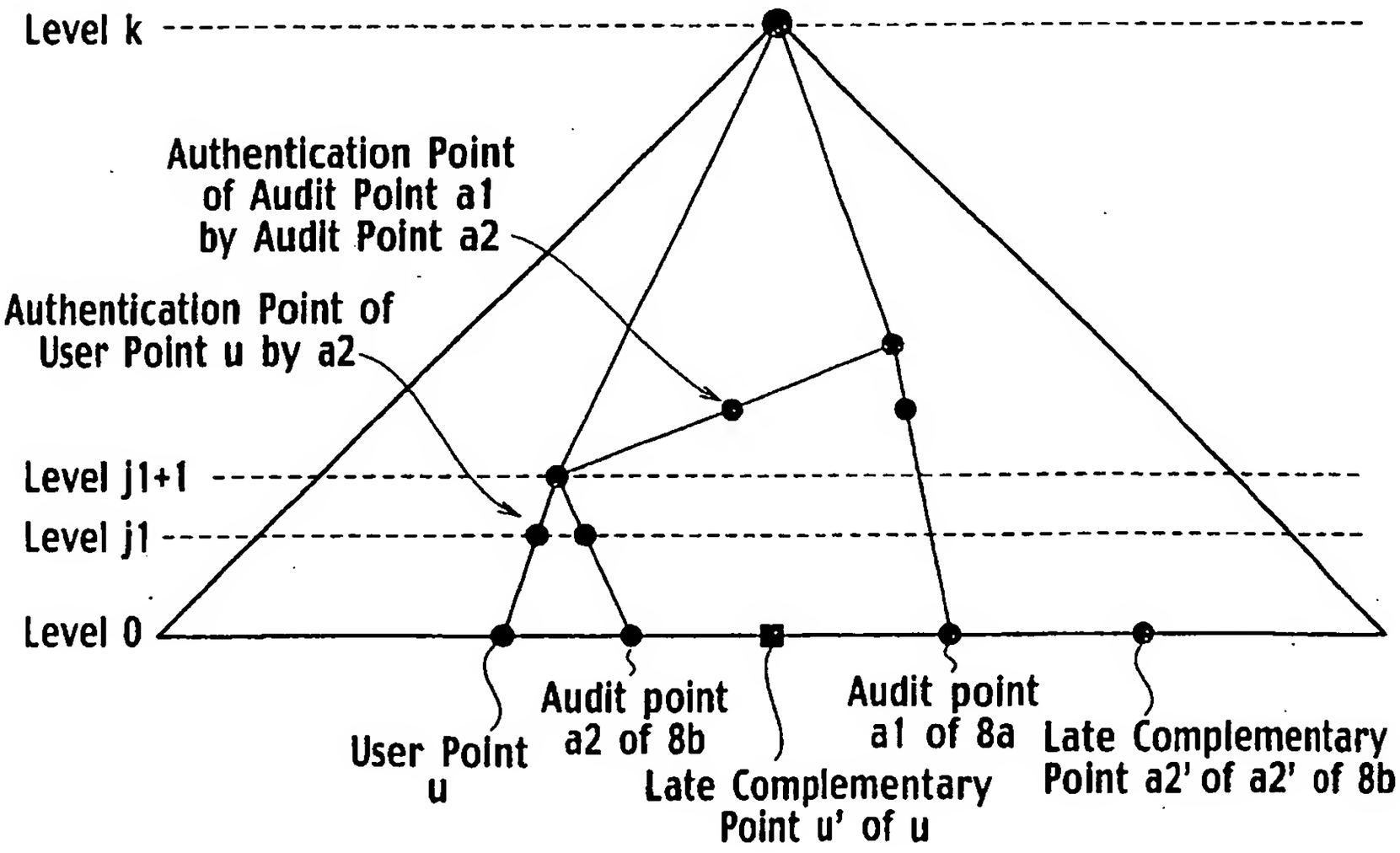

Level k
Authentication Point
of Audit Point a1
by Audit Point a2
Authentication Point of
User Point u by a2
Level j1+1
Level j1
Level 0
User Point
u
Audit point
a2 of 8b
Late Complementary
Point u' of u
Audit point
a1 of 8a
Late Complementary
Point a2' of a2' of 8b

FIG. 21

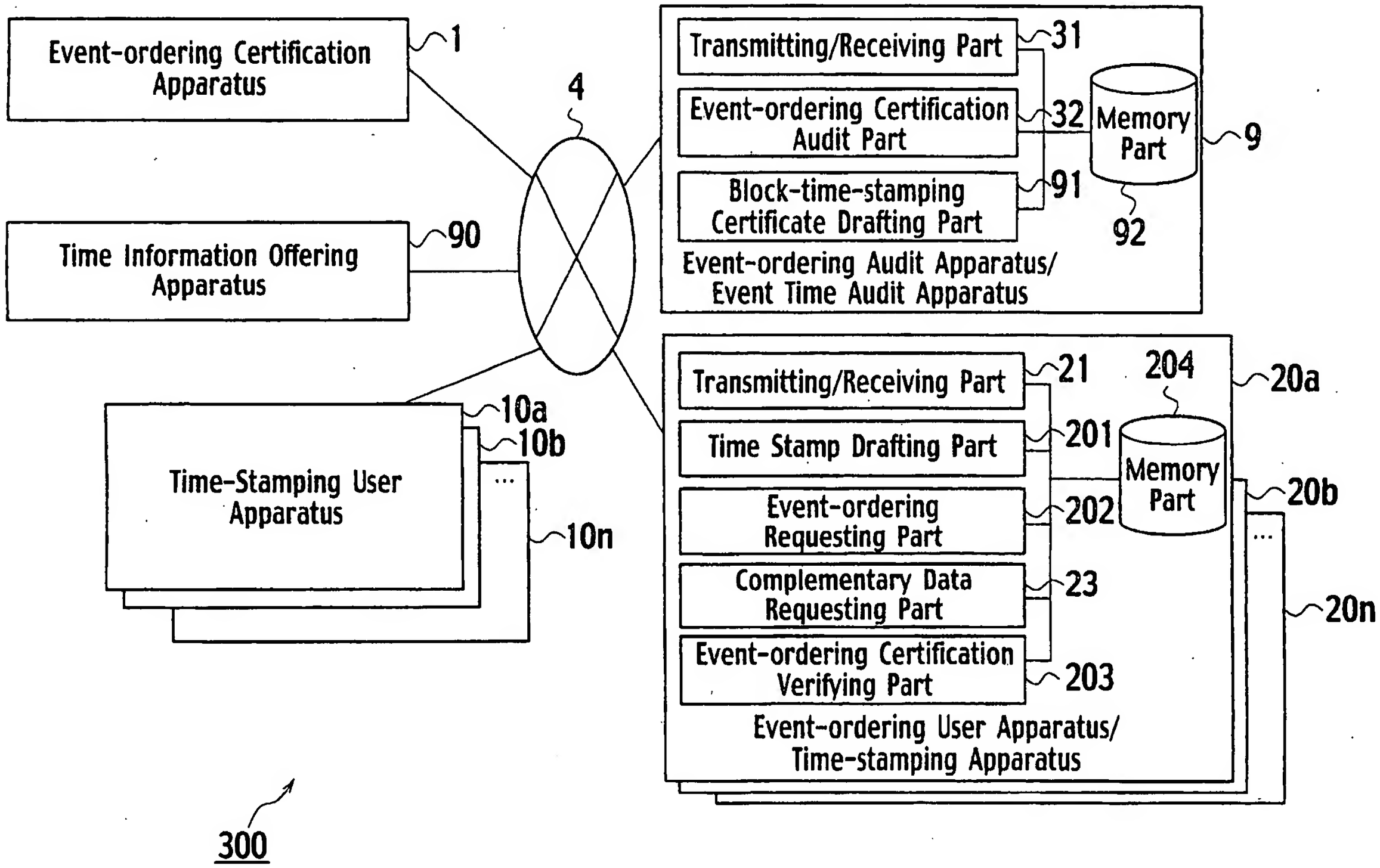

Event-ordering Certification Apparatus
1
4
Transmitting/Receiving Part
31
Event-ordering Certification Audit Part
32
Memory Part
9
Block-time-stamping Certificate Drafting Part
91
92
Event-ordering Audit Apparatus/ Event Time Audit Apparatus
Time Information Offering Apparatus
90
Time-Stamping User Apparatus
10a
10b
10n
Transmitting/Receiving Part
21
204
20a
Time Stamp Drafting Part
201
Memory Part
20b
Event-ordering Requesting Part
202
Complementary Data Requesting Part
23
20n
Event-ordering Certification Verifying Part
203
Event-ordering User Apparatus/ Time-stamping Apparatus
300

FIG. 22

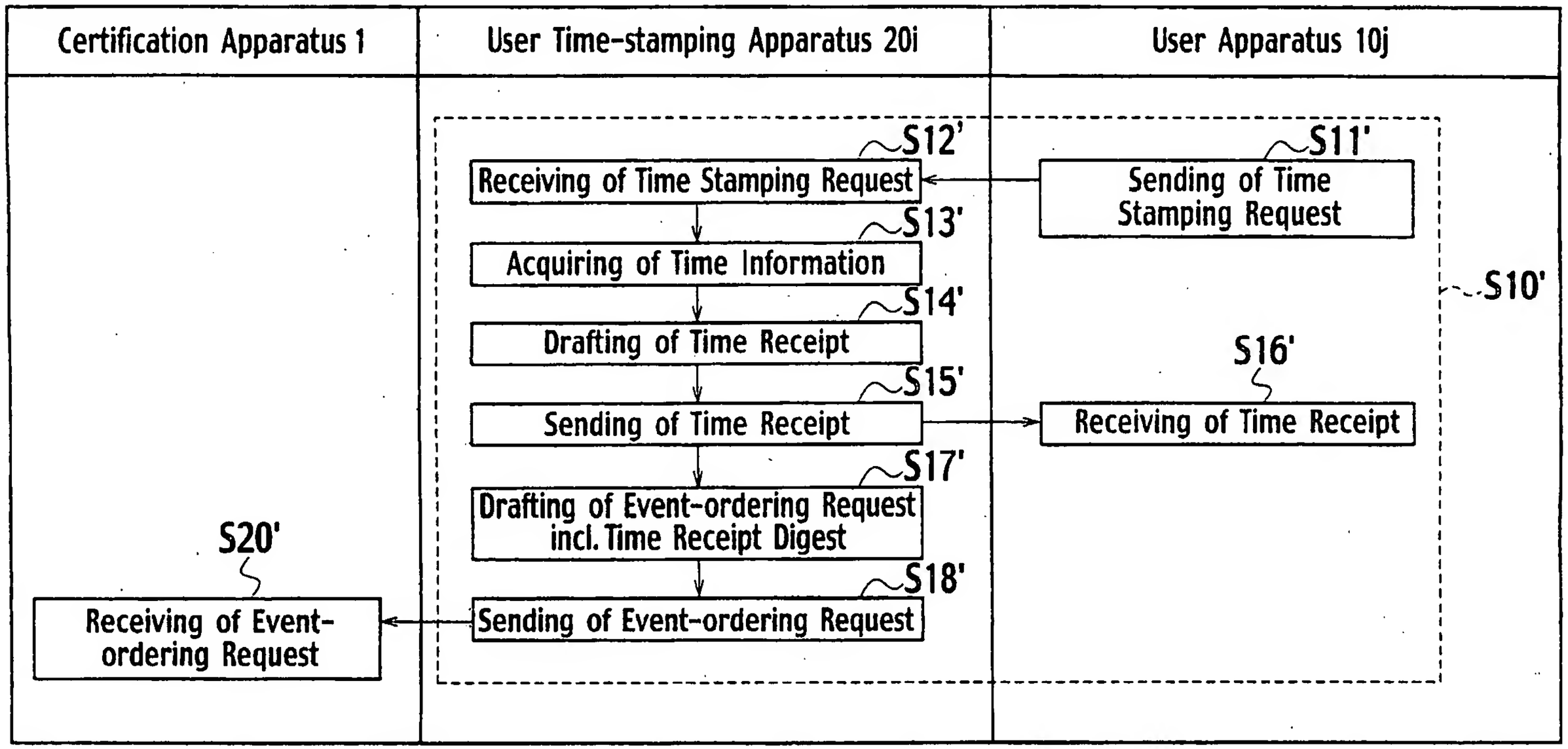

Certification Apparatus 1
User Time-stamping Apparatus 20i
User Apparatus 10j
S12'
Receiving of Time Stamping Request
S11'
Sending of Time Stamping Request
S13'
Acquiring of Time Information
S10'
S14'
Drafting of Time Receipt
S16'
S15'
Sending of Time Receipt
Receiving of Time Receipt
S17'
Drafting of Event-ordering Request incl. Time Receipt Digest
S20'
S18'
Receiving of Event-ordering Request
Sending of Event-ordering Request

FIG. 23

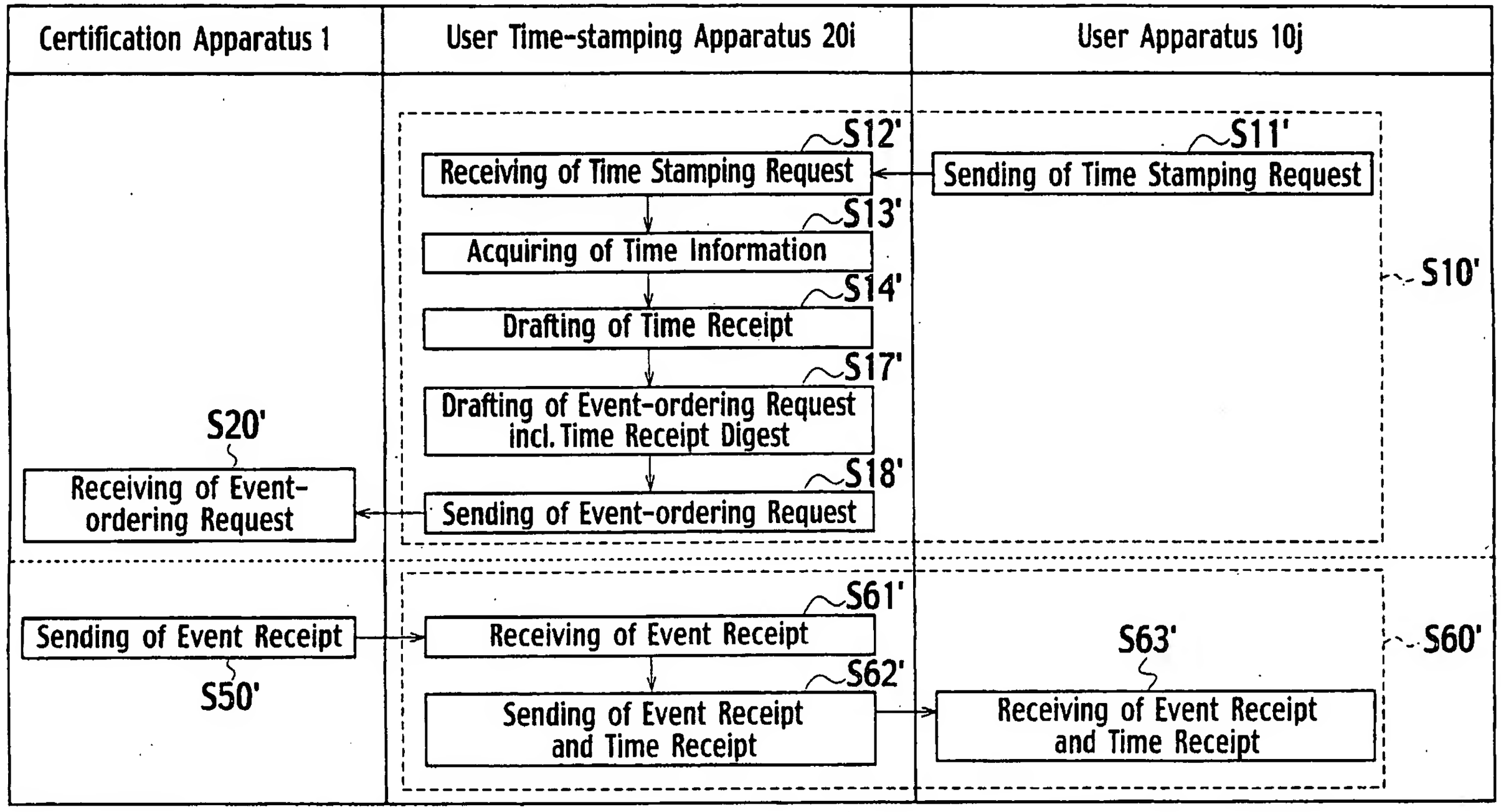

Certification Apparatus 1
User Time-stamping Apparatus 20i
User Apparatus 10j
S12'
Receiving of Time Stamping Request
S11'
Sending of Time Stamping Request
S13'
Acquiring of Time Information
S14'
Drafting of Time Receipt
S10'
S17'
Drafting of Event-ordering Request incl. Time Receipt Digest
S18'
Sending of Event-ordering Request
S20'
Receiving of Event-ordering Request
S61'
Receiving of Event Receipt
S63'
Receiving of Event Receipt and Time Receipt
S60'
S62'
Sending of Event Receipt and Time Receipt
Sending of Event Receipt
S50'

FIG. 24

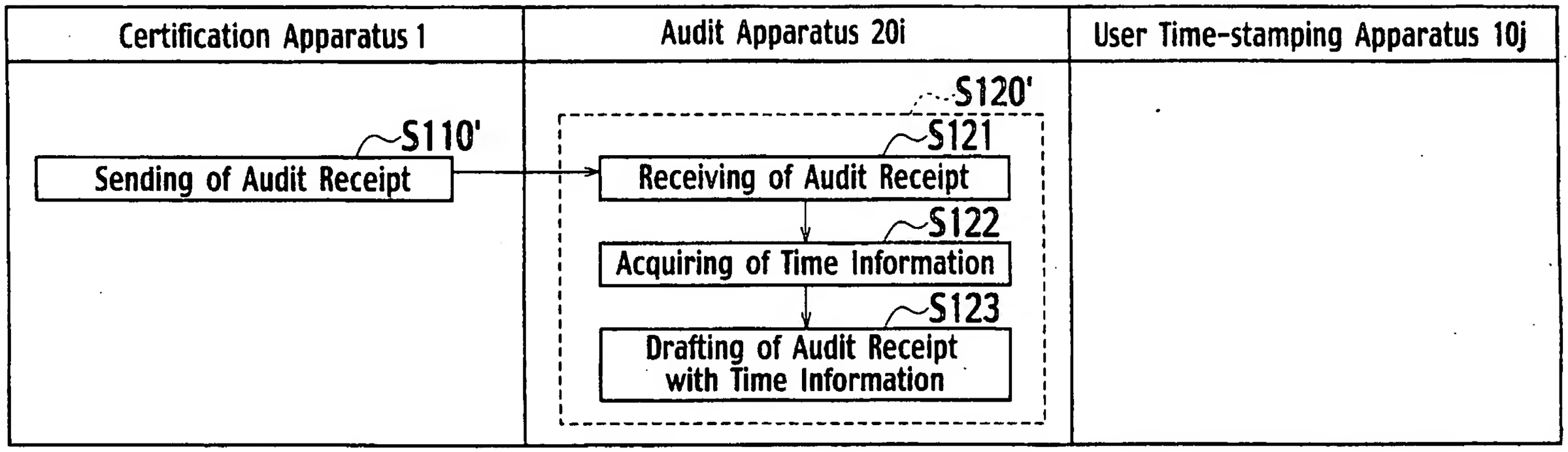

Certification Apparatus 1
Audit Apparatus 20i
User Time-stamping Apparatus 10j
S120'
S110'
Sending of Audit Receipt
S121
Receiving of Audit Receipt
S122
Acquiring of Time Information
S123
Drafting of Audit Receipt with Time Information

FIG. 25

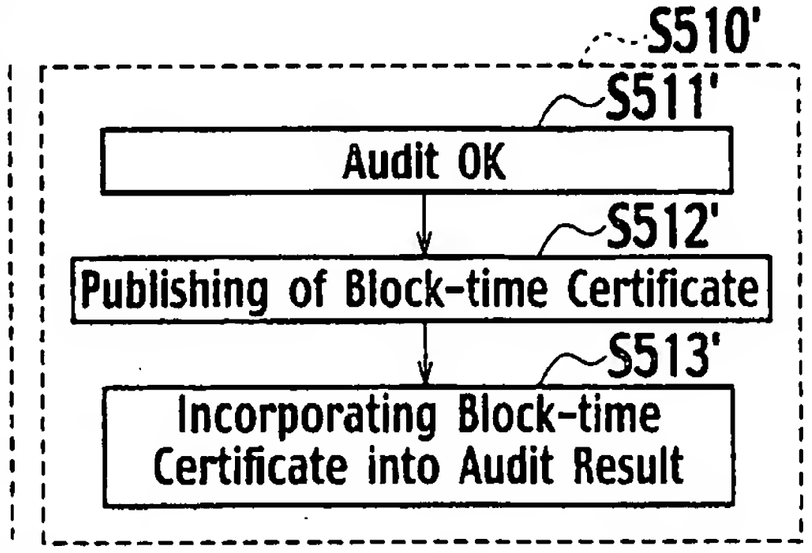
Certification Apparatus 1	Audit Apparatus 20i	User Time-stamping Apparatus 10i
		

FIG. 26

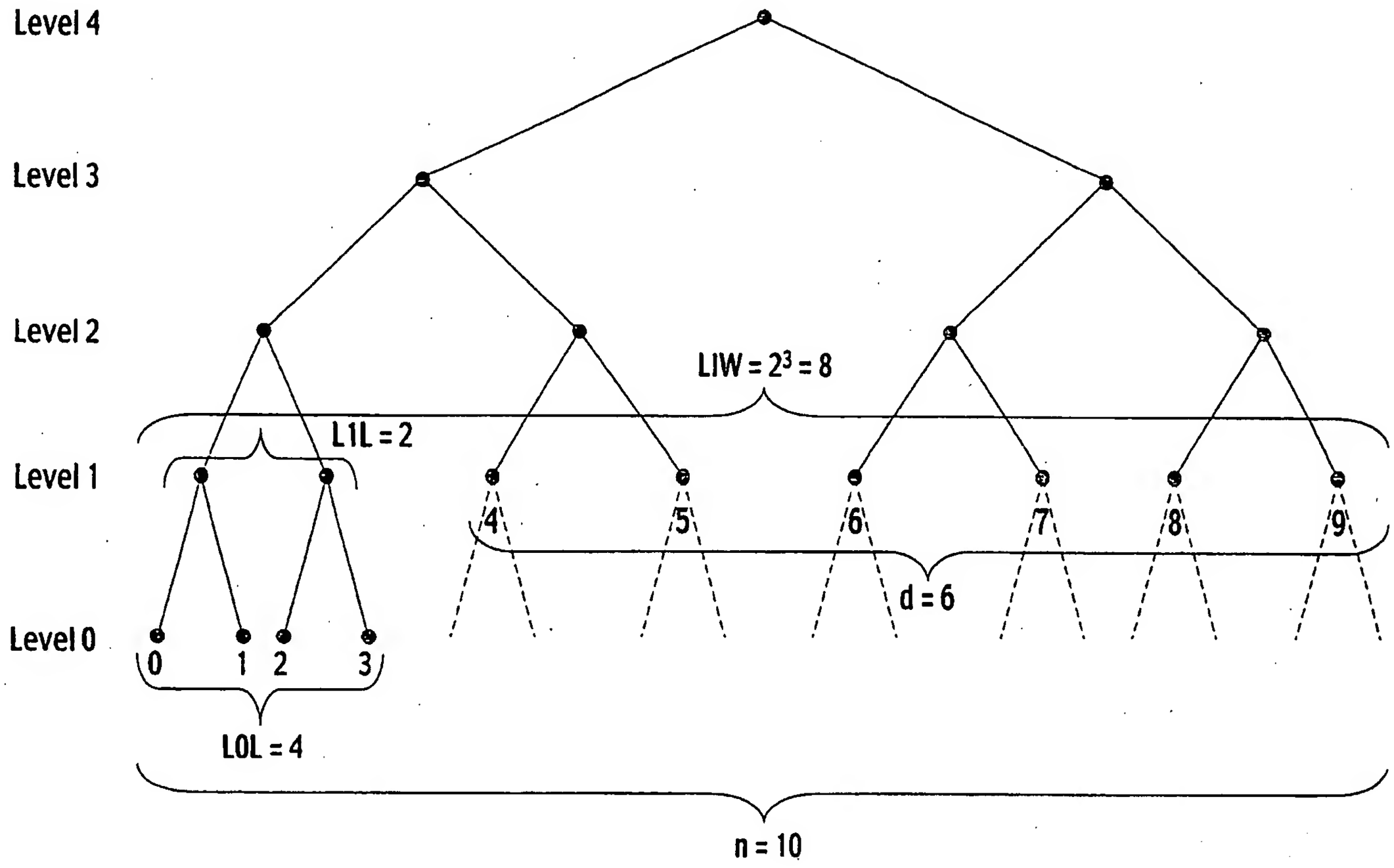

Level 4
Level 3
Level 2
Level 1
Level 0
LIW = 2^3 = 8
L1L = 2
0
1
2
3
4
5
6
7
8
9
d = 6
L0L = 4
n = 10

FIG. 27

(1) Loop 1: In a constructive method No. 3, the following processes are repeated until a regular time interval is completed.
(1.1) Setting a request on acceptance to x
(1.2) Increasing n by increment of 1
(1.3) Loop 2: Performing of the follow processes for j=0, ..., k
(1.3.1) $i \rightarrow i_j$
(1.3.2) When j = 0, set $A_j[i] := x$.
(Set x to node(j, i_j).)
(1.3.3) When j > 0, perform as follows.
· Set $x0 := A_{j-1}[index(leftChiild(j, i))]$
(Set x0 to an assigned value for left-child of node(j, i).)
· Set $x1 := A_{j-1}[index(rightChild(j, i))]$
(Set x1 to an assigned value for right-child of node(j, i).)
· Calculate $x2 := h(x0 \| x1)$
· Set $A_j[i] := x2$
(Assign x2 to node(j, i).)
(1.3.4) Increasing i_j by increment of 1
(1.3.5) Withdraw from loop 2 if i is an even number.
Completion of loop 2
Completion of loop 1

Processing Procedure 1

FIG. 28

(2) Performing of the following processes after withdrawing from loop 1 on reaching finish time.

(2.1) Set k:= ceiling($\log_2$(n)).

(2.2) Calculate rtPath(k, 0, n−1) and Set ((0, r(0), ..., k(, r(k))) to the calculation result.

(2.3) Loop 3:Performing of the follow processes for j=0, ..., k

(2.3.1) $i \rightarrow i_j$

(2.3.2) Case of j = 0:

(2.3.2.1) When i is an odd number:

- Produce a dummy r: = R(0, i)
- Set A_j[i]: = r

(Assign r to node(0, i).)

- Set b_j: = true.
- Increase i_j by increment of 1.

(2.3.2) Case of 0<j≦k:

(2.3.2.1) When i = r(j):

(when node(j, i) is on rtPath(k, 0, n−1)):

(2.3.2.1.1) x0:= A_{j-1}[index(leftChild (j, i))]

(Set x0 to an assigned value for left-child of node(j, i).)

(2.3.2.1.2) x1: = A_{j-1}[index(rightChild (j, i))]

(Set x1 to an assigned value for right-child of node(j, i).)

(2.3.2.1.3) Calculate x2: = h(x0 ‖ x1)

(2.3.2.1.4) Set A_j[i]: = x2

(Assign x2 to node(j, i).)

(2.3.2.1.5) When i is an even number and j < k:

- Increase i by increment of 1.
- Calculate r: = R(j, i) and Set A_j[i]: = r

(Assign r to node(j, i).)

- Set b_j: = true.
- Set i_j: = i + 1

(2.3.2.2) When i = r(j) + 1, an odd number and j < k:

- Calculate r: = R(j, i) and Set A_j[i]: = r

(Assign r to node(j, i).)

- Set b_j: = true.
- Increase i_j by increment of 1.

Completion of loop 3

Processing Procedure 2

FIG. 29

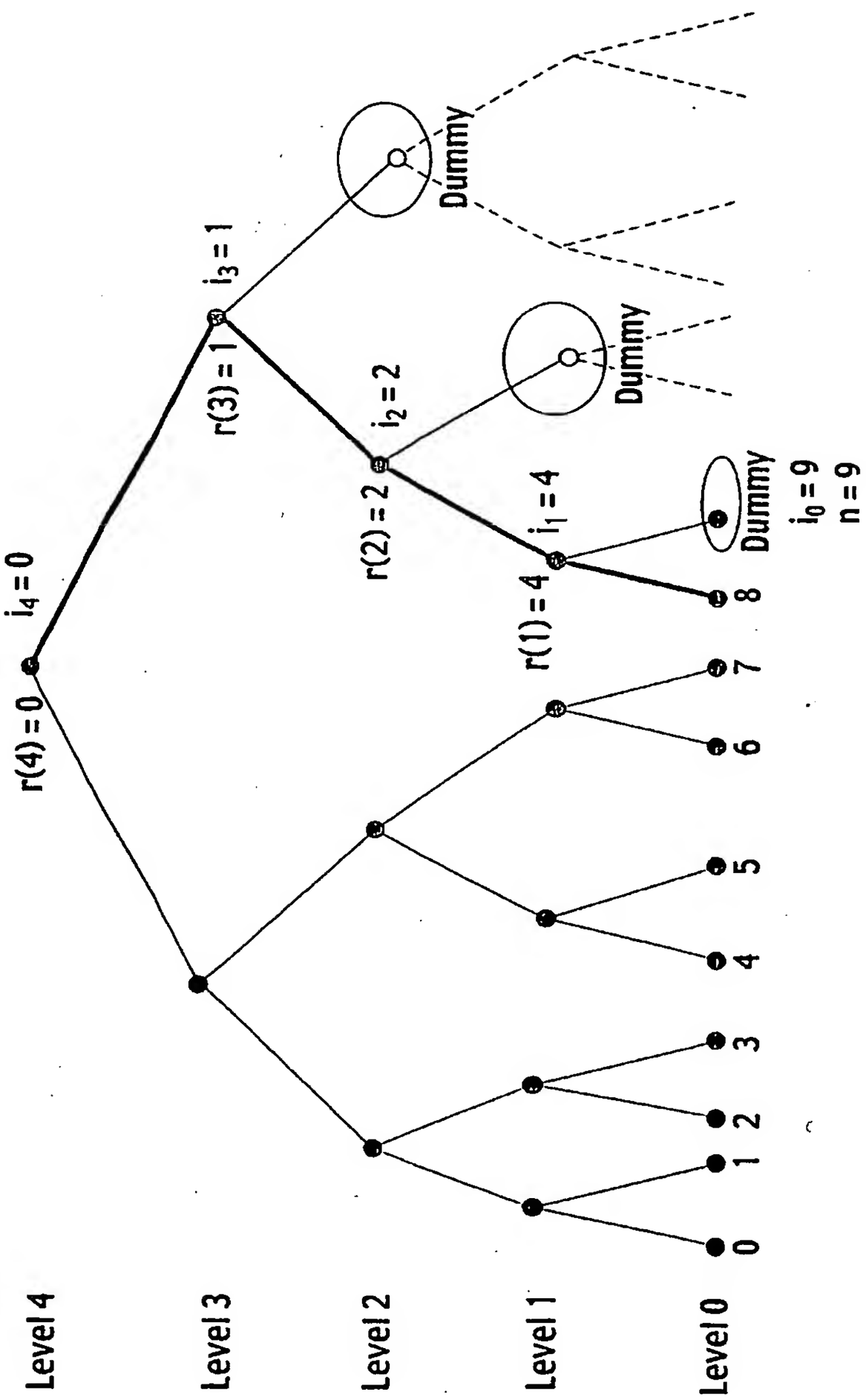

r(4) = 0
i4 = 0
r(3) = 1
i3 = 1
r(2) = 2
i2 = 2
r(1) = 4
i1 = 4
Dummy
Dummy
Dummy
i0 = 9
n = 9
0
1
2
3
4
5
6
7
8
Level 4
Level 3
Level 2
Level 1
Level 0

FIG. 30

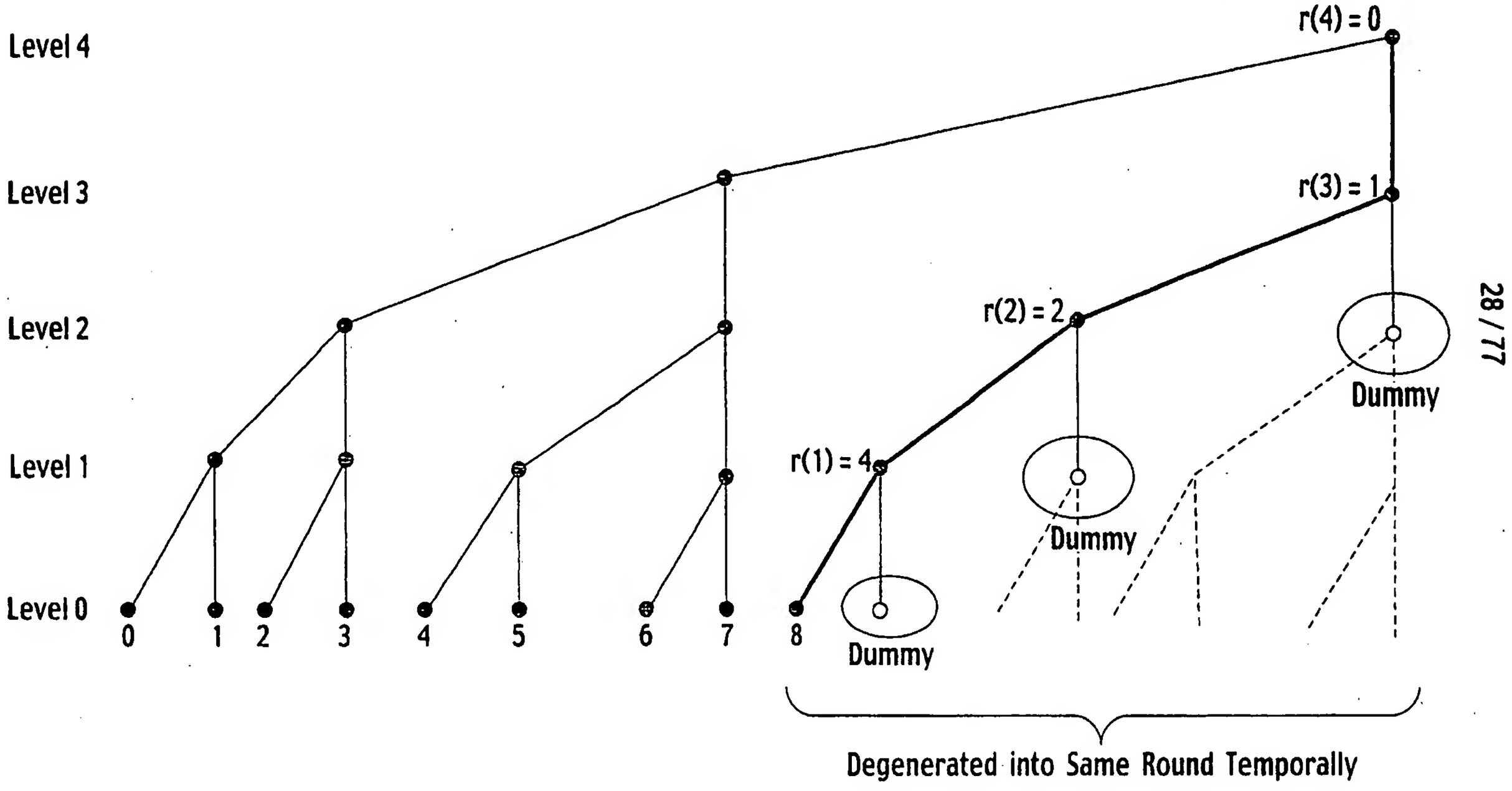

Level 4
Level 3
Level 2
Level 1
Level 0
0
1
2
3
4
5
6
7
8
r(4) = 0
r(3) = 1
r(2) = 2
r(1) = 4
Dummy
Dummy
Dummy
Degenerated into Same Round Temporally

FIG. 31

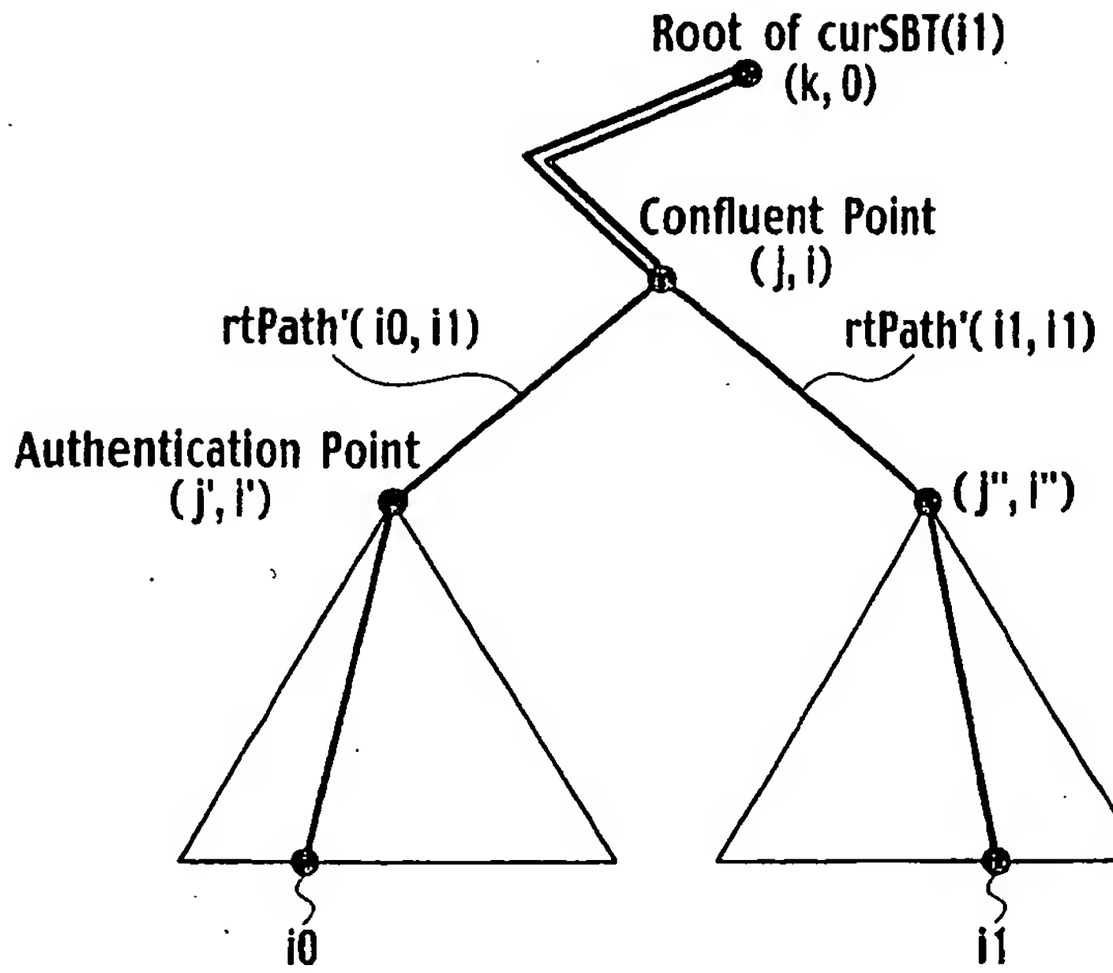

Root of curSBT(i1)
(k, 0)
Confluent Point
(j, i)
rtPath'(i0, i1)
rtPath'(i1, i1)
Authentication Point
(j', i')
(j'', i'')
i0
i1

FIG. 32

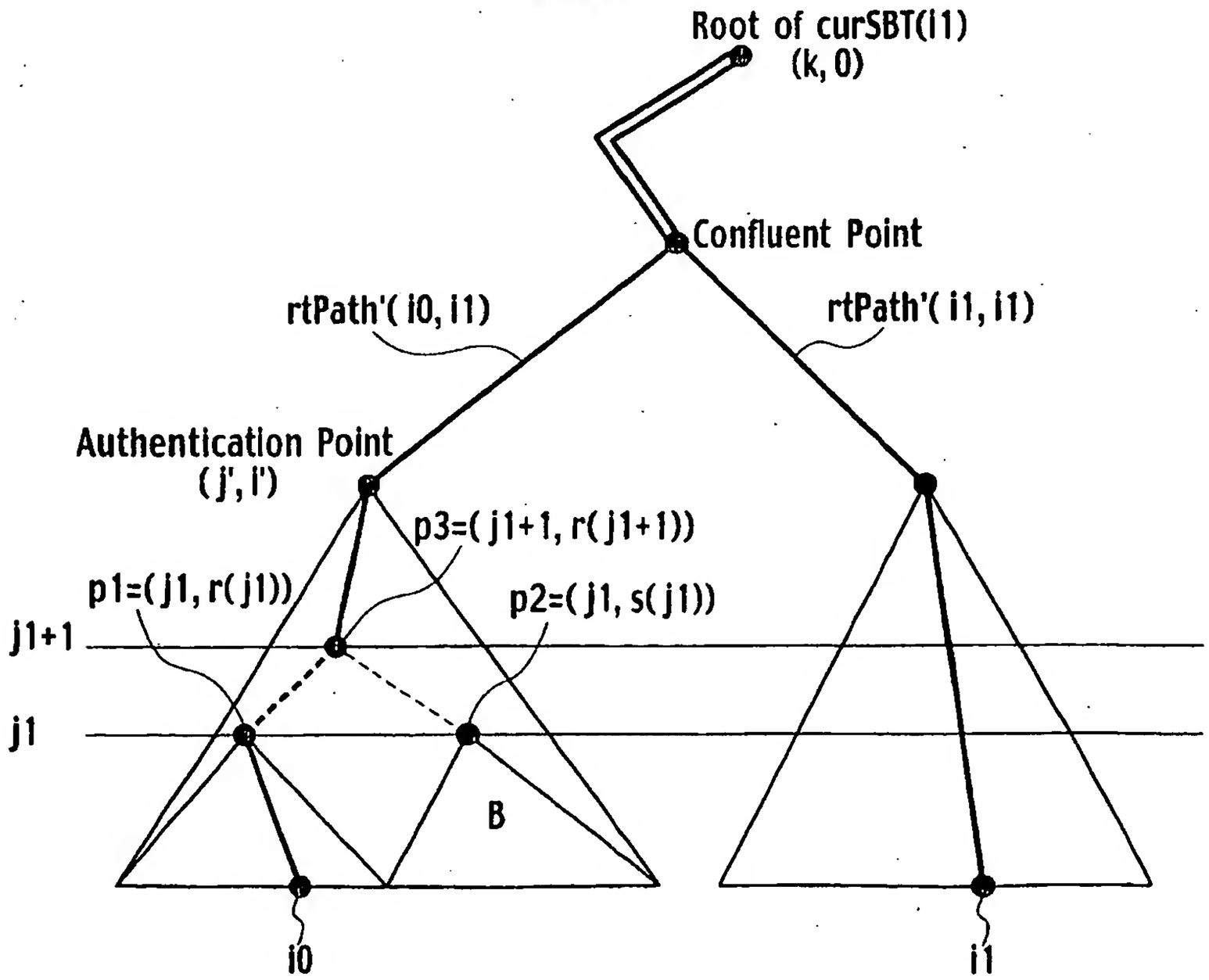

Root of curSBT(i1)
(k, 0)
Confluent Point
rtPath'(i0, i1)
rtPath'(i1, i1)
Authentication Point
(j', i')
p3=(j1+1, r(j1+1))
p1=(j1, r(j1))
p2=(j1, s(j1))
j1+1
j1
B
i0
i1

FIG. 33

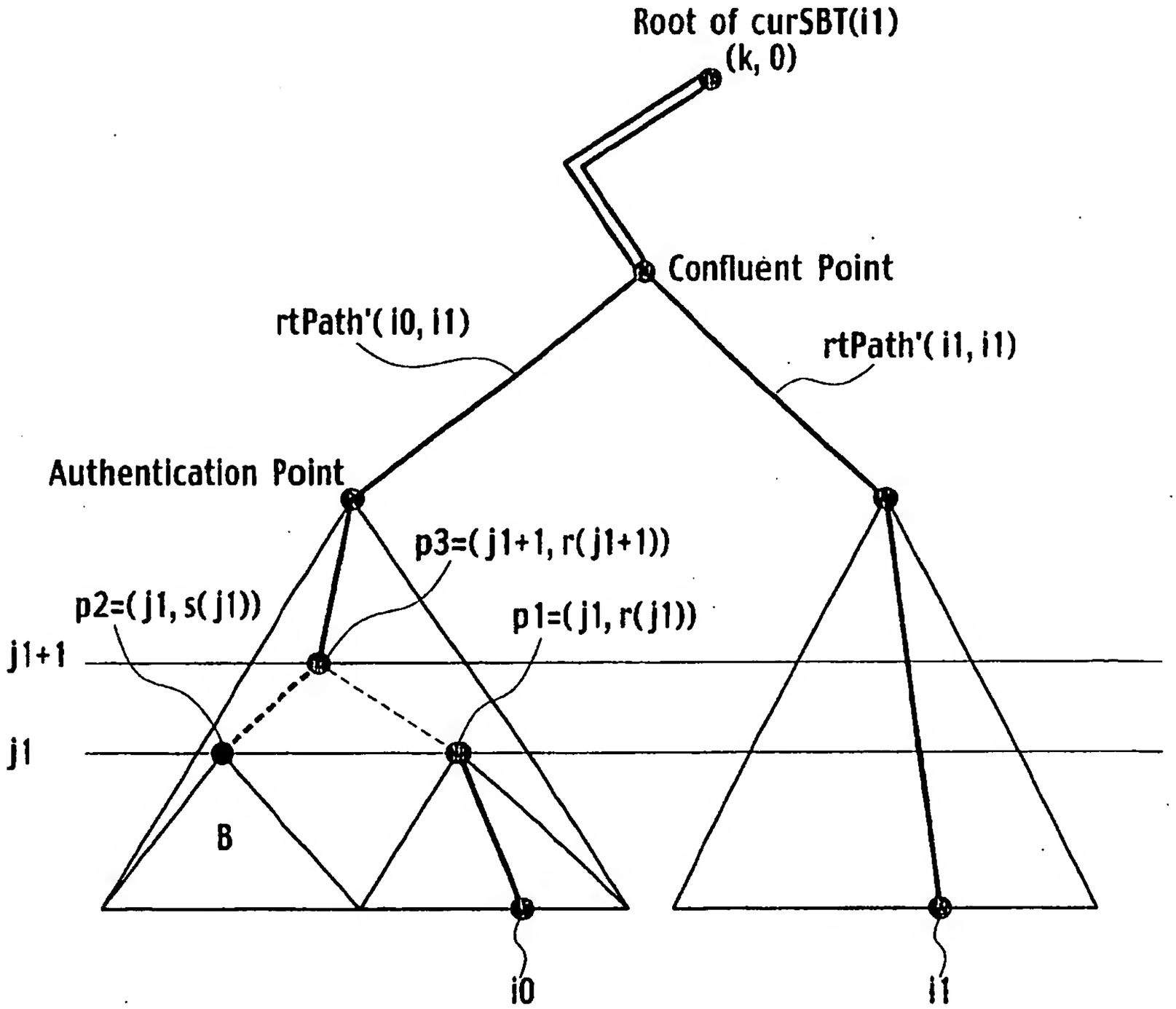

Root of curSBT(i1)
(k, 0)
Confluent Point
rtPath'(i0, i1)
rtPath'(i1, i1)
Authentication Point
p3=(j1+1, r(j1+1))
p2=(j1, s(j1))
p1=(j1, r(j1))
j1+1
j1
B
i0
i1

FIG. 34

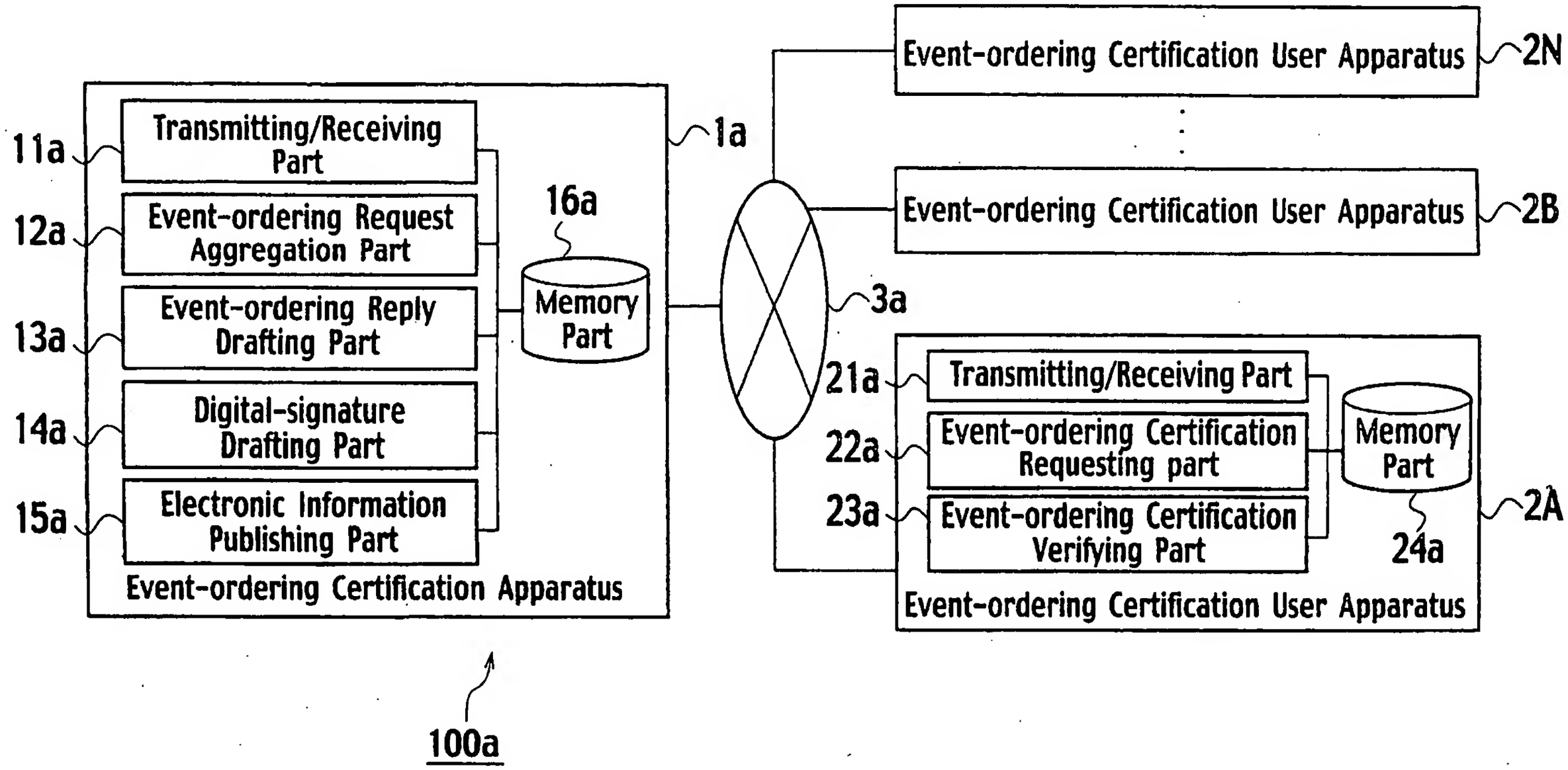

Event-ordering Certification User Apparatus
2N
Event-ordering Certification User Apparatus
2B
1a
11a
Transmitting/Receiving Part
12a
Event-ordering Request Aggregation Part
16a
13a
Event-ordering Reply Drafting Part
Memory Part
14a
Digital-signature Drafting Part
15a
Electronic Information Publishing Part
Event-ordering Certification Apparatus
3a
21a
Transmitting/Receiving Part
22a
Event-ordering Certification Requesting part
Memory Part
23a
Event-ordering Certification Verifying Part
24a
2A
Event-ordering Certification User Apparatus
100a

FIG. 35

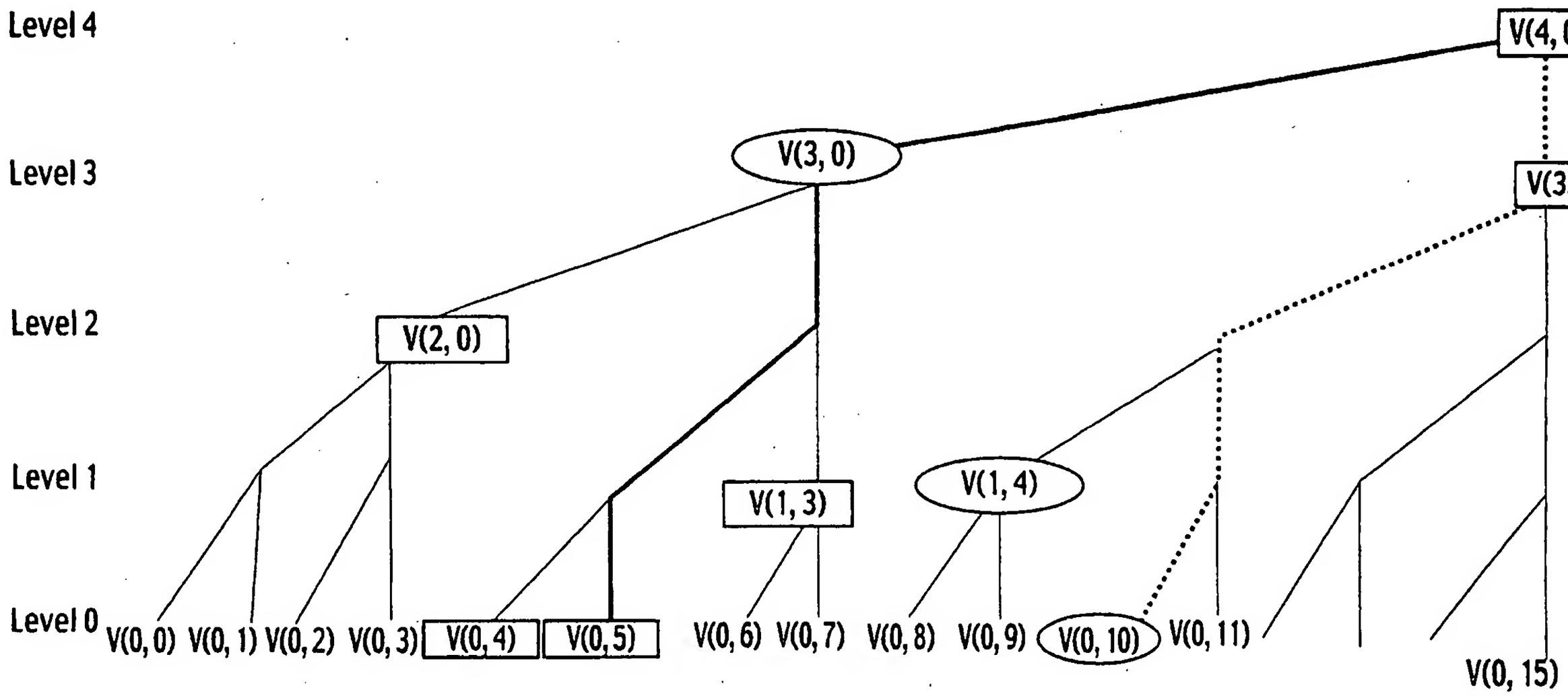
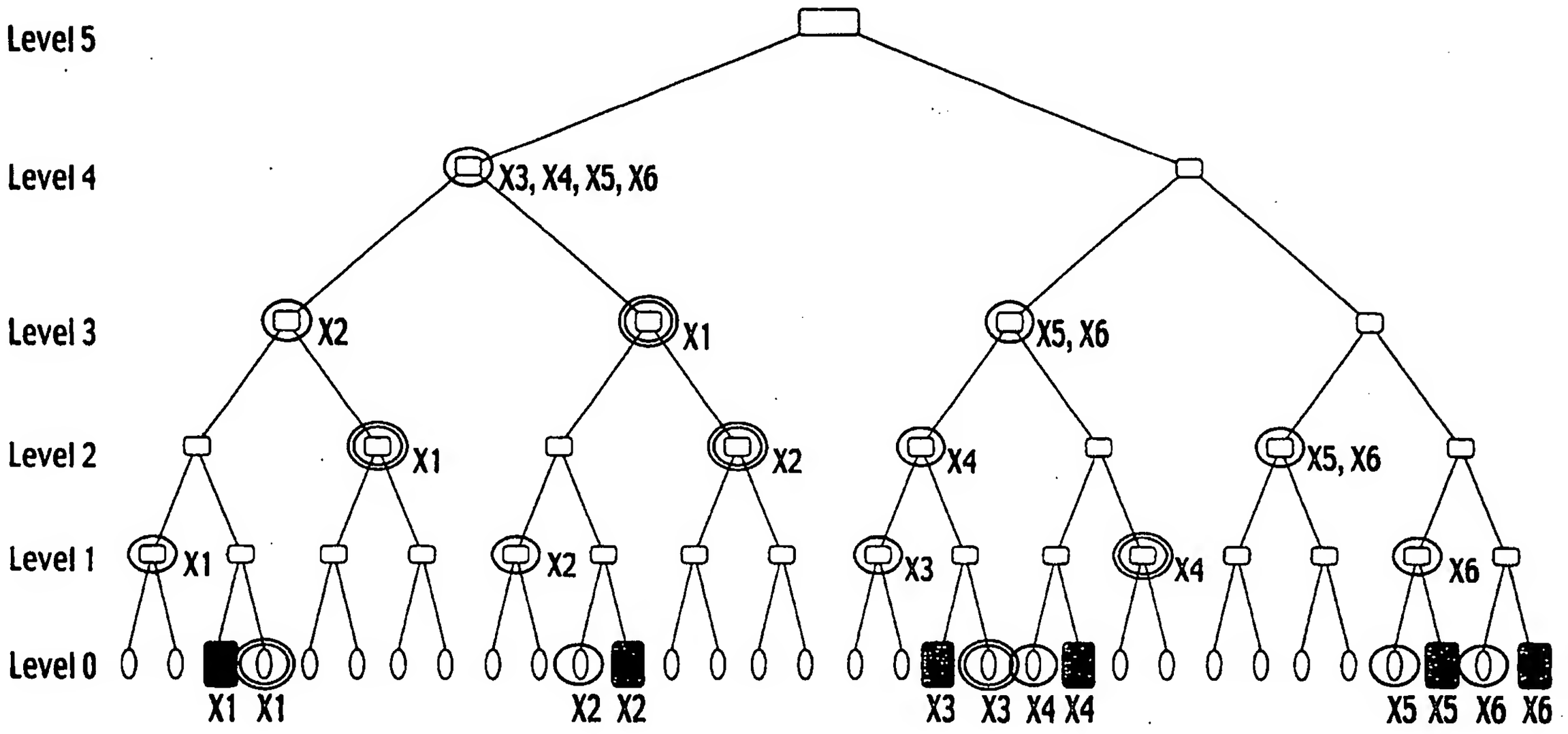

Level 4
Level 3
Level 2
Level 1
Level 0
V(4, 0)
V(3, 0)
V(3, 1)
V(2, 0)
V(1, 3)
V(1, 4)
V(0, 0)
V(0, 1)
V(0, 2)
V(0, 3)
V(0, 4)
V(0, 5)
V(0, 6)
V(0, 7)
V(0, 8)
V(0, 9)
V(0, 10)
V(0, 11)
V(0, 15)

FIG. 36

ITEM	SIGN	REQUIRED	
Original Data	y	○	Event-ordering Receipt EOC(y)
Sequentially Assigned Data-item	z	○	
Sequential Aggregation Tree No.	n	○	
Sequential Aggregation Tree Leaf No.	i	○	
Immediate Complementary Data of Registration Point (Positional Information Assigned Value)	SK	○	
Late Complementary Data of Each Past Registration Point (Positional Information Assigned Value)	TK	○	

FIG. 37



: Requested Registration Point X (X=X1, X2, X3, X4, X5, X6)

: Requested Registration Point X : Immediate Complementary Data

: Requested Registration Point X : Late Complementary Data

FIG. 38

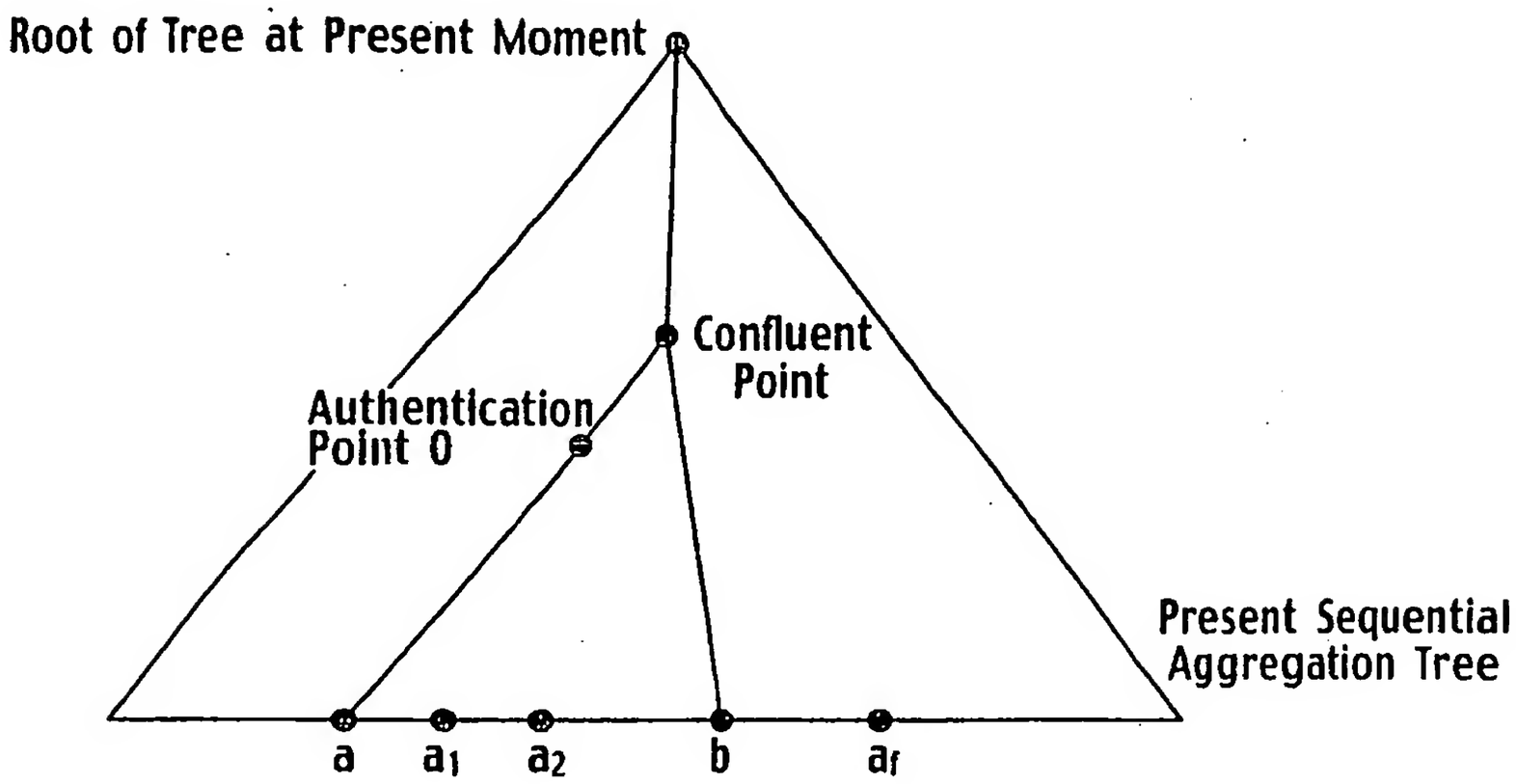

Root of Tree at Present Moment
Confluent Point
Authentication Point 0
Present Sequential Aggregation Tree
a
a1
a2
b
af

FIG. 39

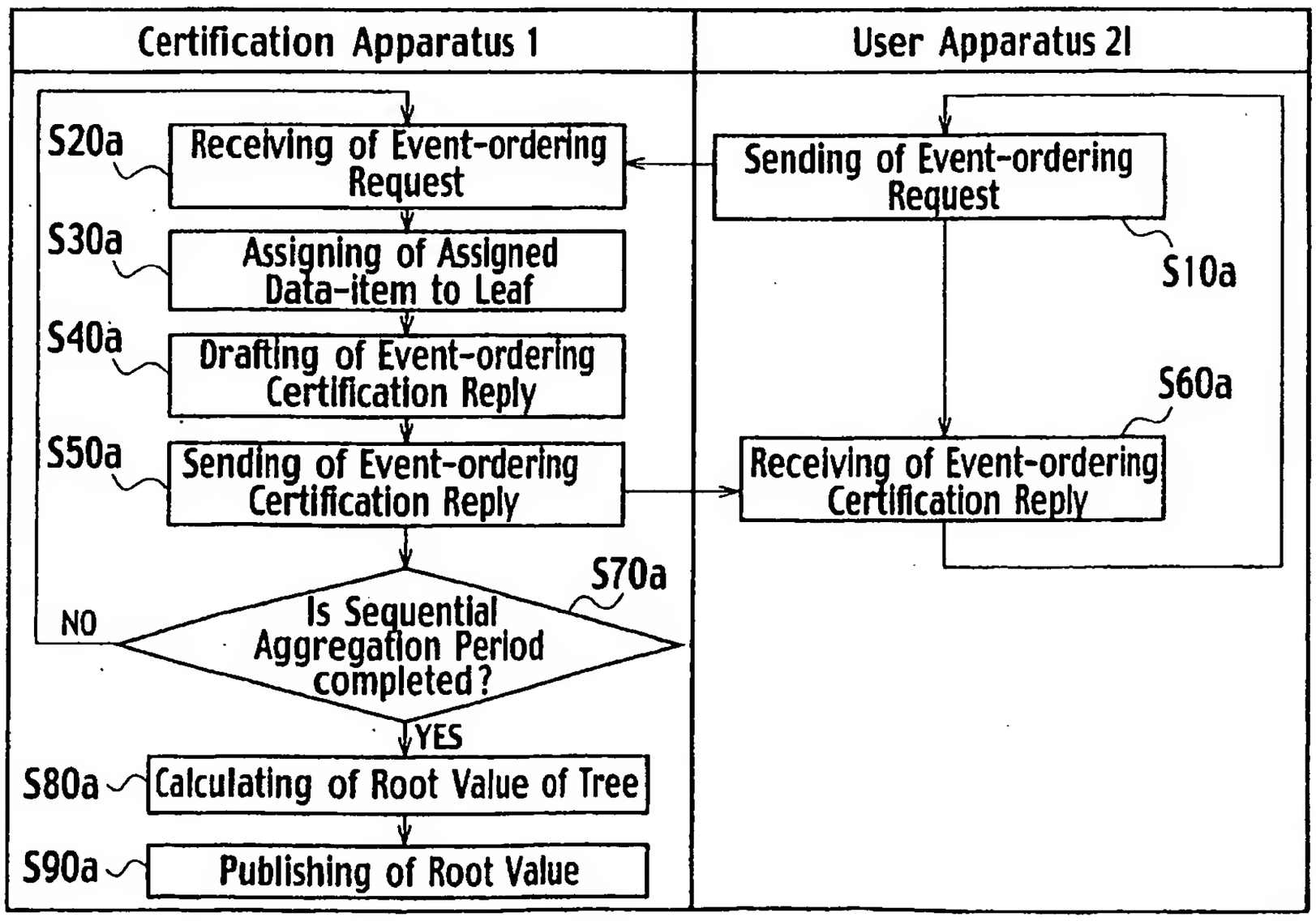

Certification Apparatus 1
User Apparatus 2l
S20a
Receiving of Event-ordering Request
S30a
Assigning of Assigned Data-item to Leaf
S40a
Drafting of Event-ordering Certification Reply
S50a
Sending of Event-ordering Certification Reply
S70a
Is Sequential Aggregation Period completed?
NO
YES
S80a
Calculating of Root Value of Tree
S90a
Publishing of Root Value
Sending of Event-ordering Request
S10a
S60a
Receiving of Event-ordering Certification Reply

FIG. 40

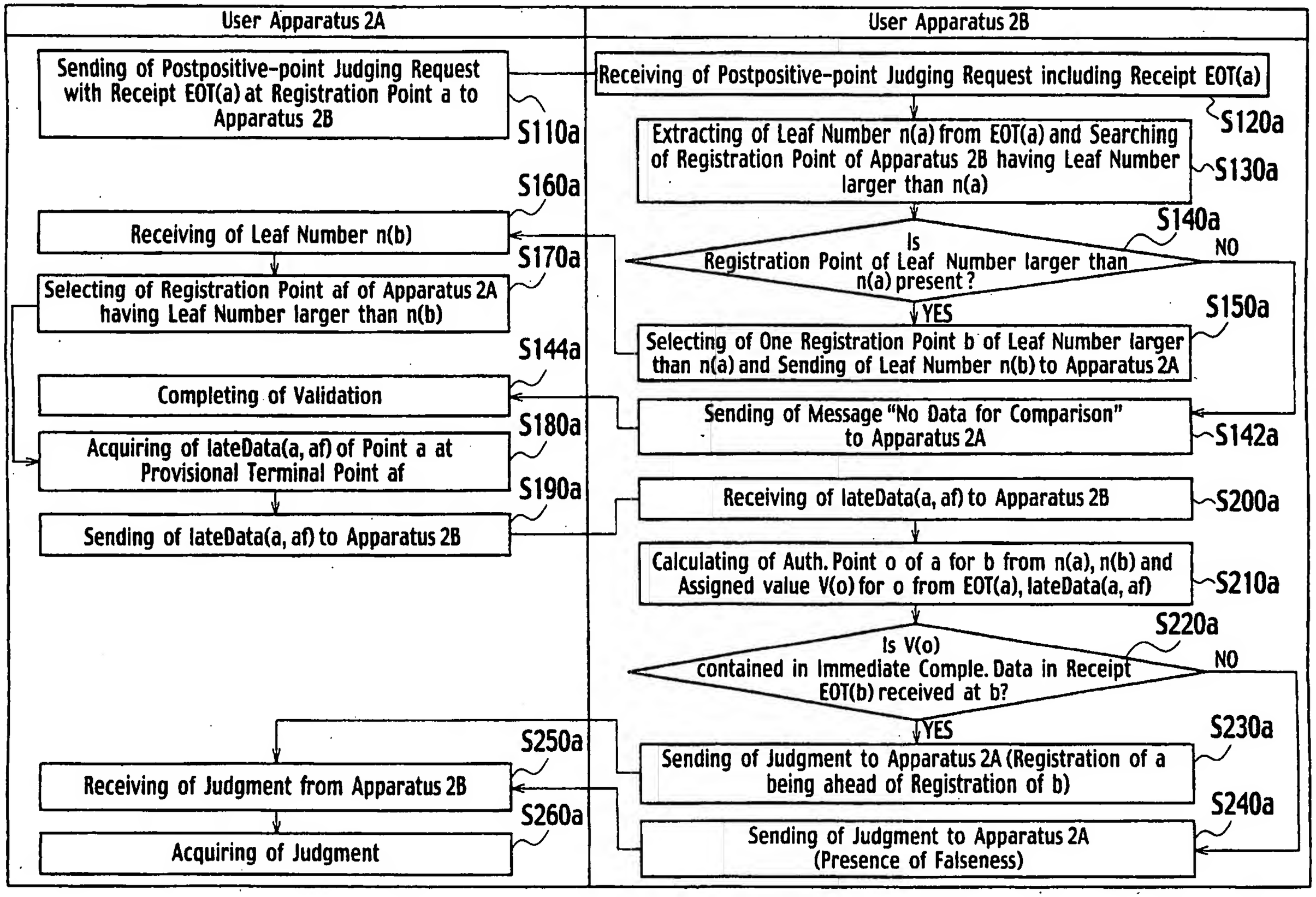

User Apparatus 2A
User Apparatus 2B
Sending of Postpositive-point Judging Request with Receipt EOT(a) at Registration Point a to Apparatus 2B
S110a
Receiving of Postpositive-point Judging Request including Receipt EOT(a)
S120a
Extracting of Leaf Number n(a) from EOT(a) and Searching of Registration Point of Apparatus 2B having Leaf Number larger than n(a)
S130a
S140a
Is Registration Point of Leaf Number larger than n(a) present?
NO
YES
S150a
Selecting of One Registration Point b of Leaf Number larger than n(a) and Sending of Leaf Number n(b) to Apparatus 2A
S160a
Receiving of Leaf Number n(b)
S170a
Selecting of Registration Point af of Apparatus 2A having Leaf Number larger than n(b)
S144a
Completing of Validation
Sending of Message "No Data for Comparison" to Apparatus 2A
S142a
S180a
Acquiring of lateData(a, af) of Point a at Provisional Terminal Point af
S190a
Sending of lateData(a, af) to Apparatus 2B
Receiving of lateData(a, af) to Apparatus 2B
S200a
Calculating of Auth. Point o of a for b from n(a), n(b) and Assigned value V(o) for o from EOT(a), lateData(a, af)
S210a
S220a
Is V(o) contained in Immediate Comple. Data in Receipt EOT(b) received at b?
NO
YES
S230a
Sending of Judgment to Apparatus 2A (Registration of a being ahead of Registration of b)
S250a
Receiving of Judgment from Apparatus 2B
S240a
Sending of Judgment to Apparatus 2A (Presence of Falseness)
S260a
Acquiring of Judgment

FIG. 41

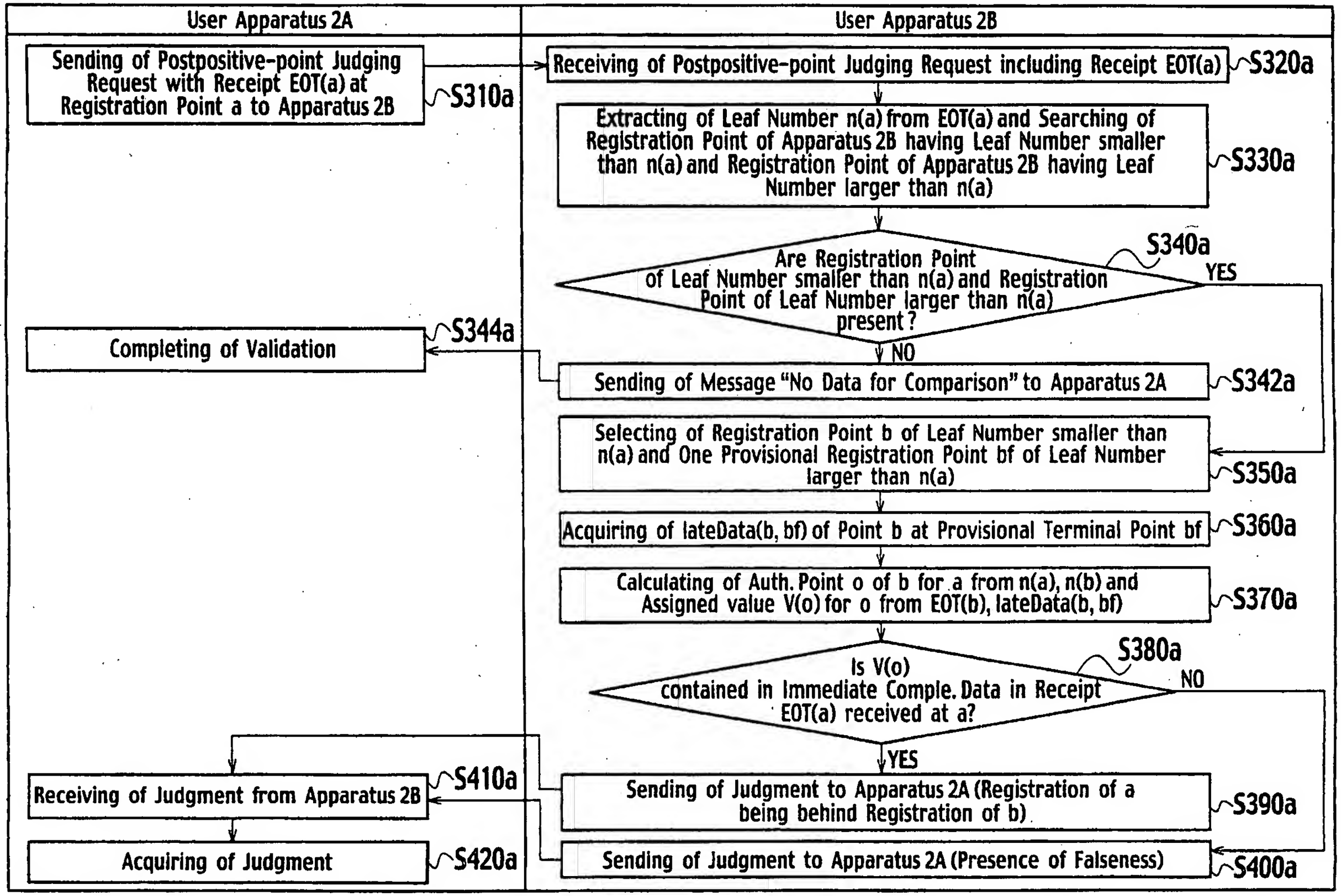

User Apparatus 2A
User Apparatus 2B
Sending of Postpositive-point Judging Request with Receipt EOT(a) at Registration Point a to Apparatus 2B
S310a
Receiving of Postpositive-point Judging Request including Receipt EOT(a)
S320a
Extracting of Leaf Number n(a) from EOT(a) and Searching of Registration Point of Apparatus 2B having Leaf Number smaller than n(a) and Registration Point of Apparatus 2B having Leaf Number larger than n(a)
S330a
Are Registration Point of Leaf Number smaller than n(a) and Registration Point of Leaf Number larger than n(a) present?
S340a
YES
NO
Completing of Validation
S344a
Sending of Message "No Data for Comparison" to Apparatus 2A
S342a
Selecting of Registration Point b of Leaf Number smaller than n(a) and One Provisional Registration Point bf of Leaf Number larger than n(a)
S350a
Acquiring of lateData(b, bf) of Point b at Provisional Terminal Point bf
S360a
Calculating of Auth. Point o of b for a from n(a), n(b) and Assigned value V(o) for o from EOT(b), lateData(b, bf)
S370a
Is V(o) contained in Immediate Comple. Data in Receipt EOT(a) received at a?
S380a
NO
YES
Receiving of Judgment from Apparatus 2B
S410a
Sending of Judgment to Apparatus 2A (Registration of a being behind Registration of b)
S390a
Acquiring of Judgment
S420a
Sending of Judgment to Apparatus 2A (Presence of Falseness)
S400a

FIG. 42

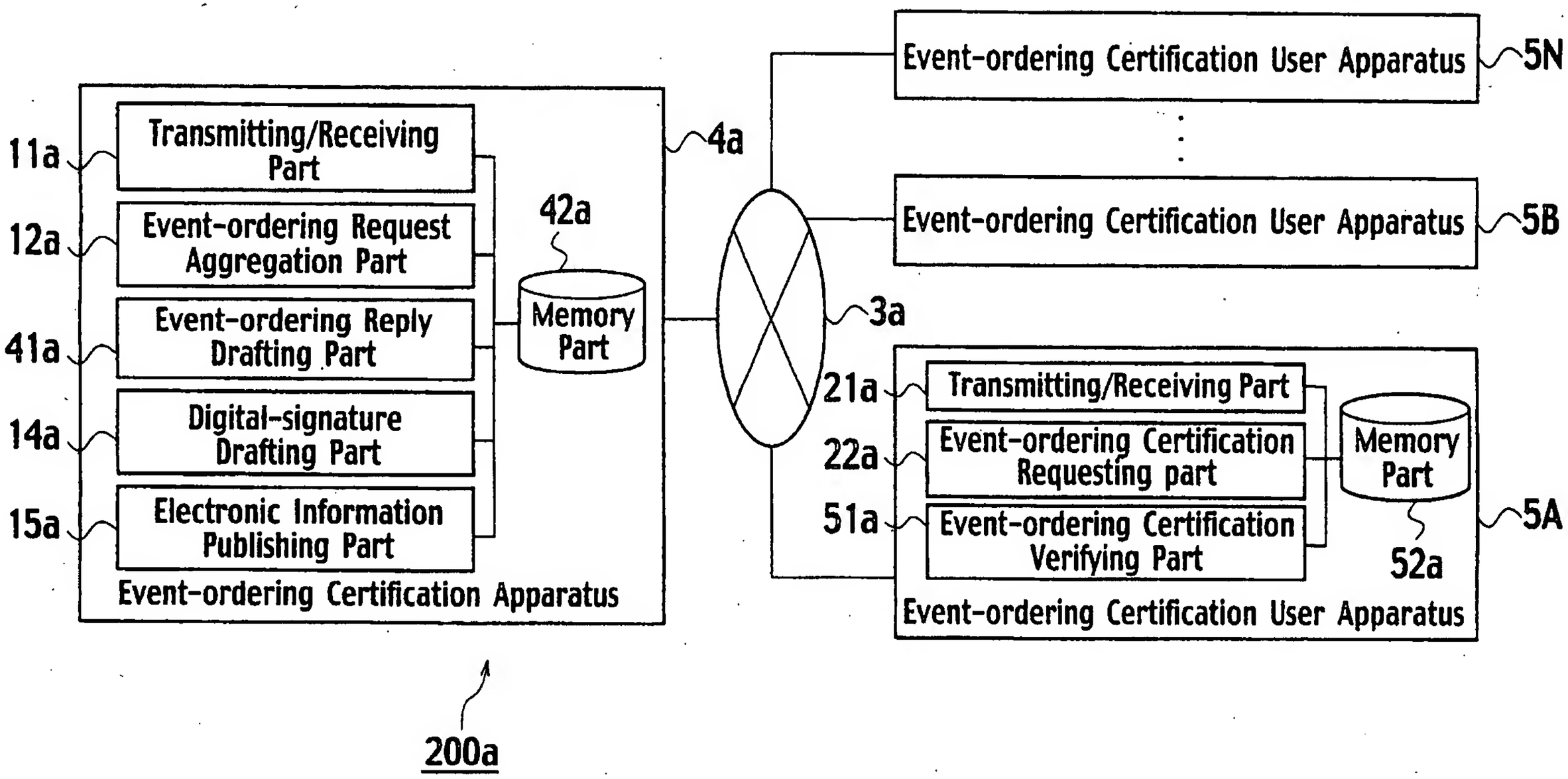
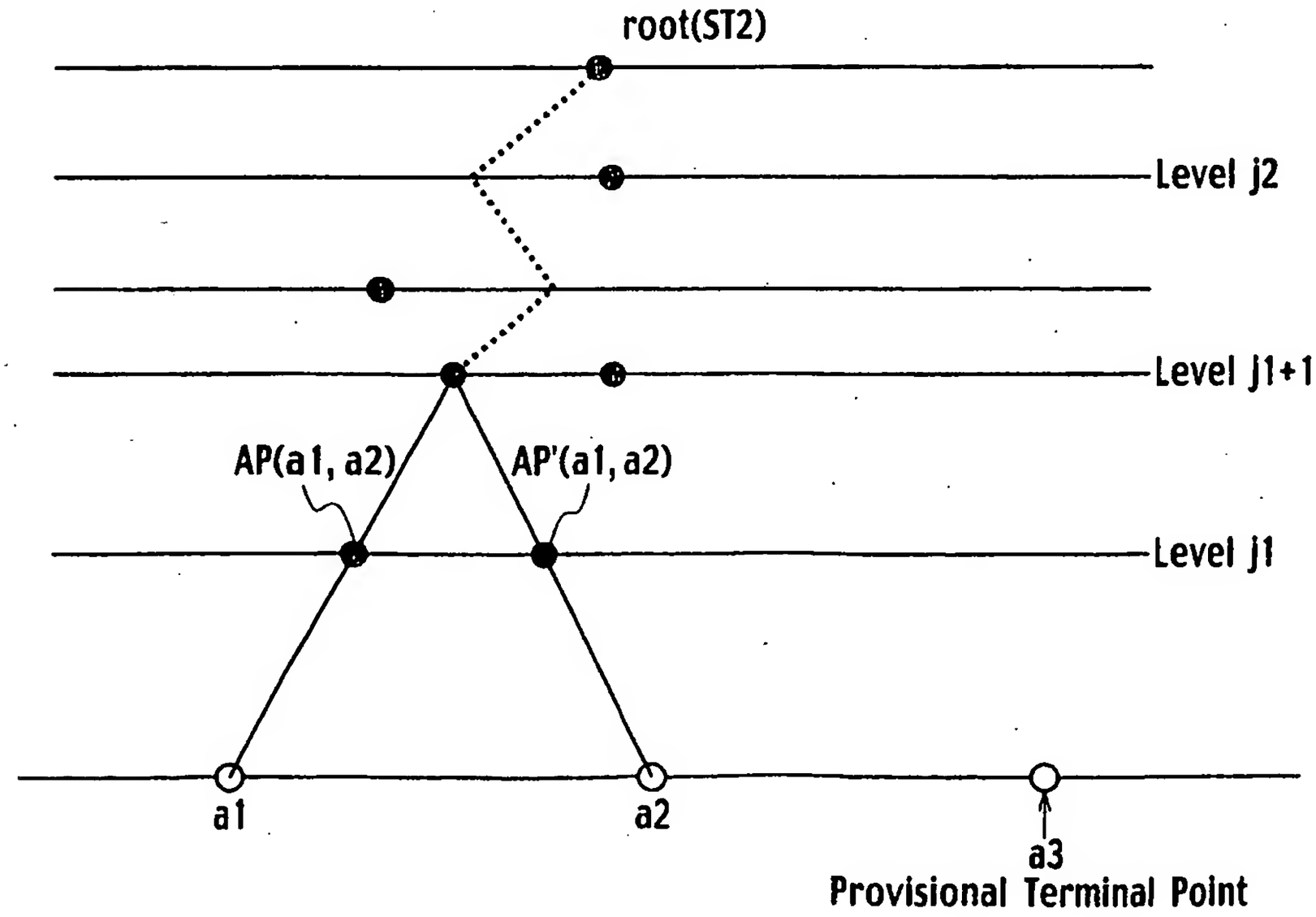

Event-ordering Certification User Apparatus
5N
Event-ordering Certification User Apparatus
5B
4a
11a
Transmitting/Receiving Part
12a
Event-ordering Request Aggregation Part
42a
Memory Part
41a
Event-ordering Reply Drafting Part
14a
Digital-signature Drafting Part
15a
Electronic Information Publishing Part
Event-ordering Certification Apparatus
3a
21a
Transmitting/Receiving Part
22a
Event-ordering Certification Requesting part
51a
Event-ordering Certification Verifying Part
Memory Part
52a
5A
Event-ordering Certification User Apparatus
200a

FIG. 43

ITEM	SIGN	REQUIRED
Original Data	y	○
Sequentially Assigned Data-item	z	○
Sequential Aggregation Tree No.	n	○
Sequential Aggregation Tree Leaf No.	i	○
Immediate Complementary Data of Registration Point (Positional Information Assigned Value)	SK	○
Late Complementary Data of Immediately-preceding Registration Point (Positional Information Assigned Value)	TK2	○

Event-ordering Receipt EOC(y)

FIG. 44



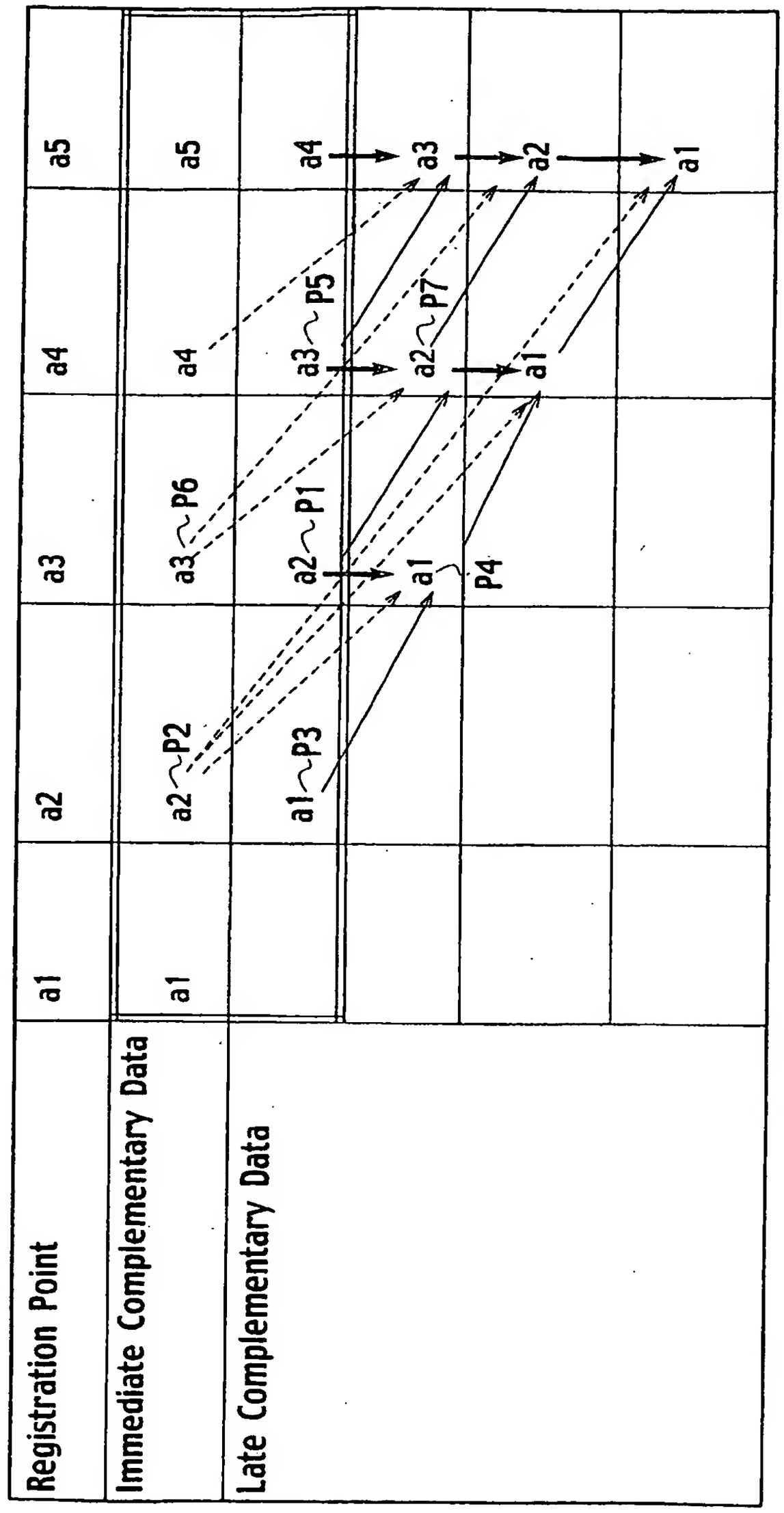
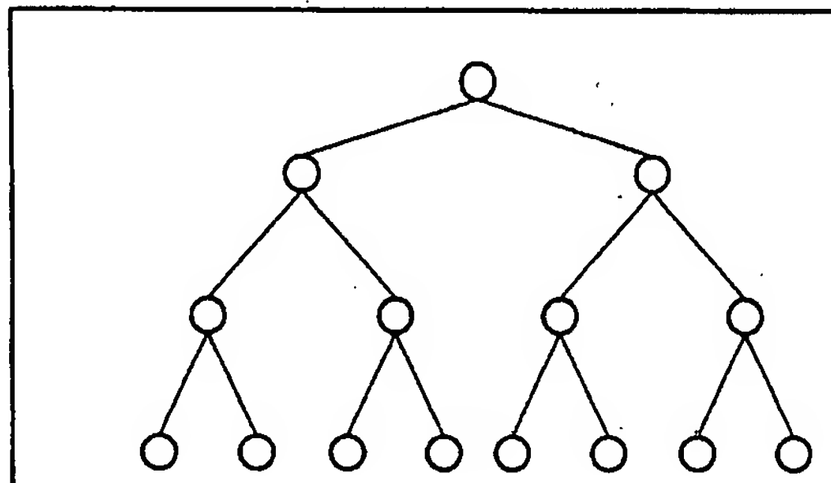

a5
a5
a4
a3
a2
a1
a4
a4
a3~P5
a2~P7
a1
a3
a3~P6
a2~P1
a1
P4
a2
a2~P2
a1~P3
a1
a1
Registration Point
Immediate Complementary Data
Late Complementary Data

FIG. 45

FIG. 46



Storing of Nodes having Requests Assigned, Positional Information and Assigned Values for Calculable Nodes

Immediately-preceding Registration Point of User Apparatus 5A
Immediately-preceding Registration Point of User Apparatus 5B
Immediately-preceding Registration Point of User Apparatus 5C
⋮
Immediately-preceding Registration Point of User Apparatus 5N
⋮

Memory Part 42a

FIG. 47

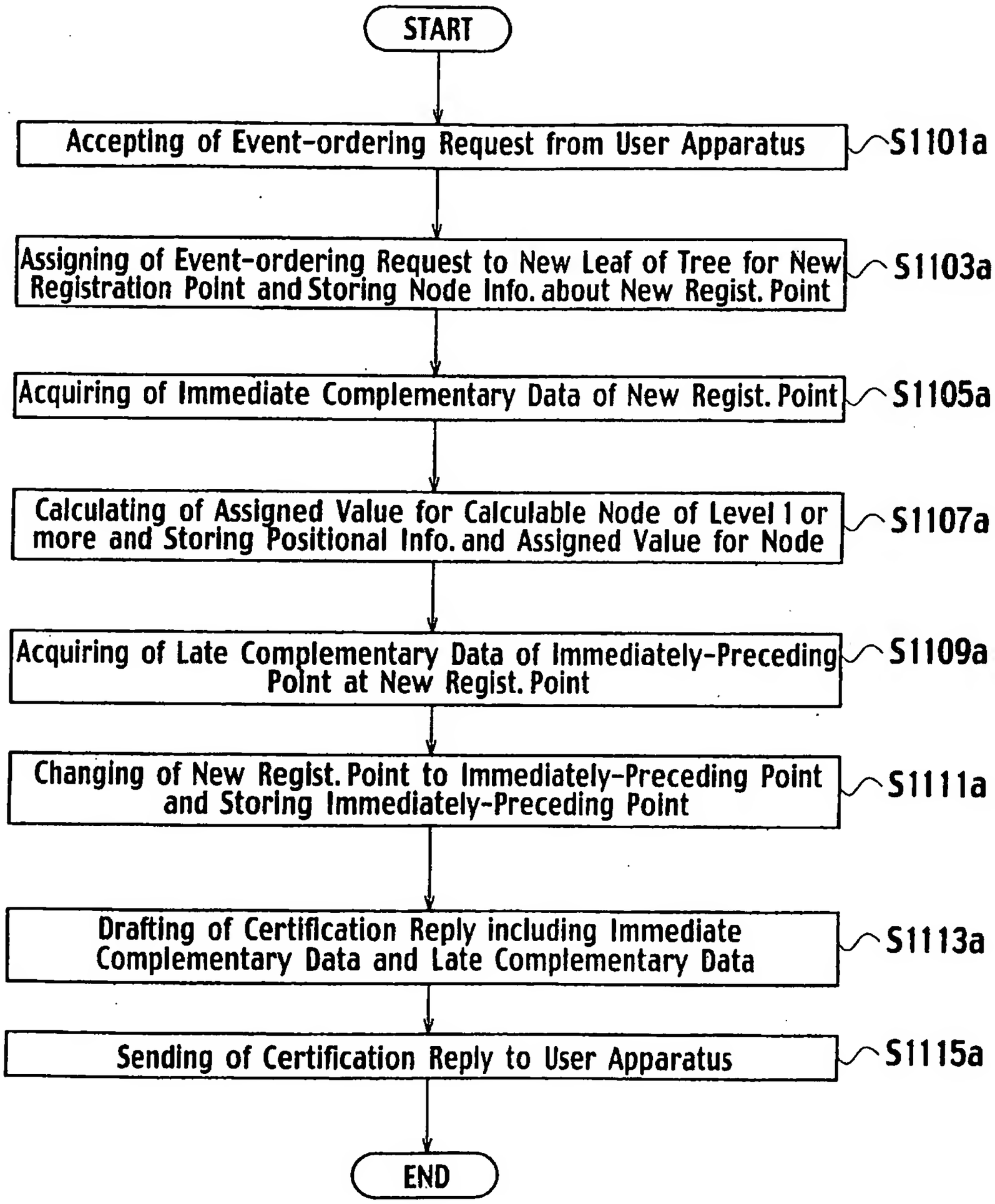

START
Accepting of Event-ordering Request from User Apparatus
S1101a
Assigning of Event-ordering Request to New Leaf of Tree for New Registration Point and Storing Node Info. about New Regist. Point
S1103a
Acquiring of Immediate Complementary Data of New Regist. Point
S1105a
Calculating of Assigned Value for Calculable Node of Level 1 or more and Storing Positional Info. and Assigned Value for Node
S1107a
Acquiring of Late Complementary Data of Immediately-Preceding Point at New Regist. Point
S1109a
Changing of New Regist. Point to Immediately-Preceding Point and Storing Immediately-Preceding Point
S1111a
Drafting of Certification Reply including Immediate Complementary Data and Late Complementary Data
S1113a
Sending of Certification Reply to User Apparatus
S1115a
END

FIG. 48

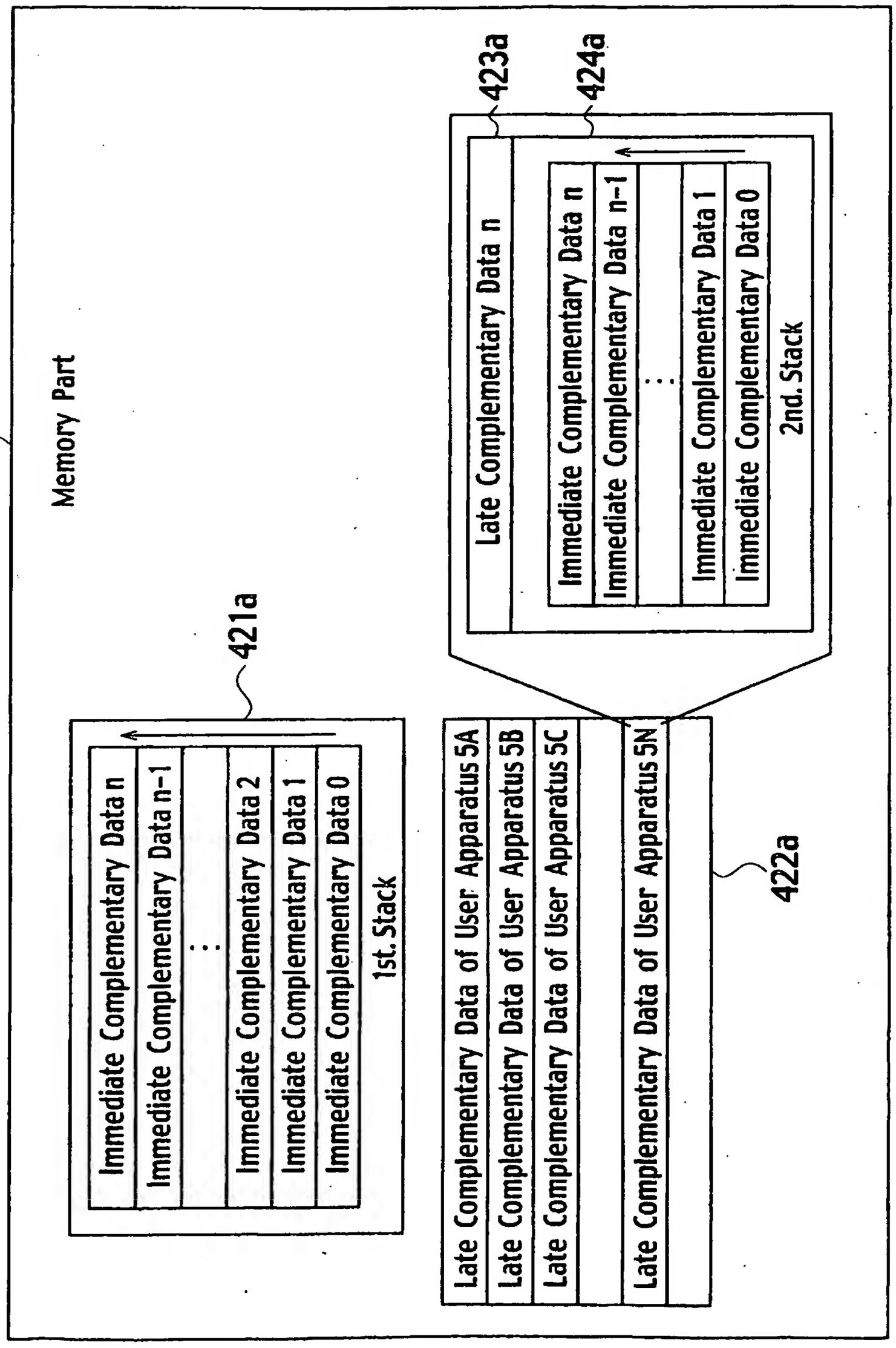

42a
Memory Part
421a
Immediate Complementary Data n
Immediate Complementary Data n-1
Immediate Complementary Data 2
Immediate Complementary Data 1
Immediate Complementary Data 0
1st. Stack
422a
Late Complementary Data of User Apparatus 5A
Late Complementary Data of User Apparatus 5B
Late Complementary Data of User Apparatus 5C
Late Complementary Data of User Apparatus 5N
423a
424a
Late Complementary Data n
Immediate Complementary Data m
Immediate Complementary Data n-1
Immediate Complementary Data 1
Immediate Complementary Data 0
2nd. Stack

FIG. 49

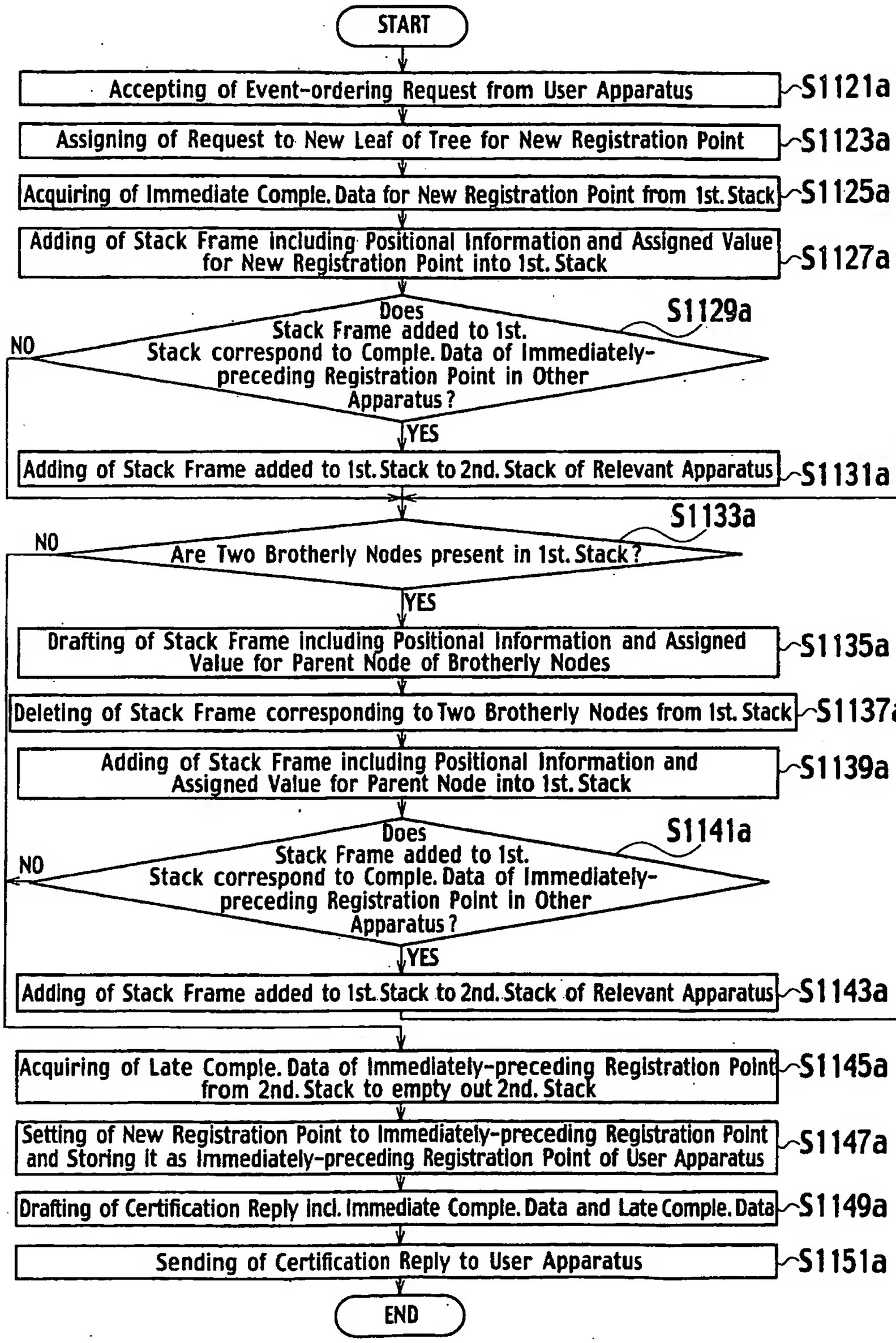

START
Accepting of Event-ordering Request from User Apparatus
S1121a
Assigning of Request to New Leaf of Tree for New Registration Point
S1123a
Acquiring of Immediate Comple. Data for New Registration Point from 1st. Stack
S1125a
Adding of Stack Frame including Positional Information and Assigned Value for New Registration Point into 1st. Stack
S1127a
Does Stack Frame added to 1st. Stack correspond to Comple. Data of Immediately-preceding Registration Point in Other Apparatus?
S1129a
NO
YES
Adding of Stack Frame added to 1st. Stack to 2nd. Stack of Relevant Apparatus
S1131a
Are Two Brotherly Nodes present in 1st. Stack?
S1133a
NO
YES
Drafting of Stack Frame including Positional Information and Assigned Value for Parent Node of Brotherly Nodes
S1135a
Deleting of Stack Frame corresponding to Two Brotherly Nodes from 1st. Stack
S1137a
Adding of Stack Frame including Positional Information and Assigned Value for Parent Node into 1st. Stack
S1139a
Does Stack Frame added to 1st. Stack correspond to Comple. Data of Immediately-preceding Registration Point in Other Apparatus?
S1141a
NO
YES
Adding of Stack Frame added to 1st. Stack to 2nd. Stack of Relevant Apparatus
S1143a
Acquiring of Late Comple. Data of Immediately-preceding Registration Point from 2nd. Stack to empty out 2nd. Stack
S1145a
Setting of New Registration Point to Immediately-preceding Registration Point and Storing it as Immediately-preceding Registration Point of User Apparatus
S1147a
Drafting of Certification Reply Incl. Immediate Comple. Data and Late Comple. Data
S1149a
Sending of Certification Reply to User Apparatus
S1151a
END

FIG. 50

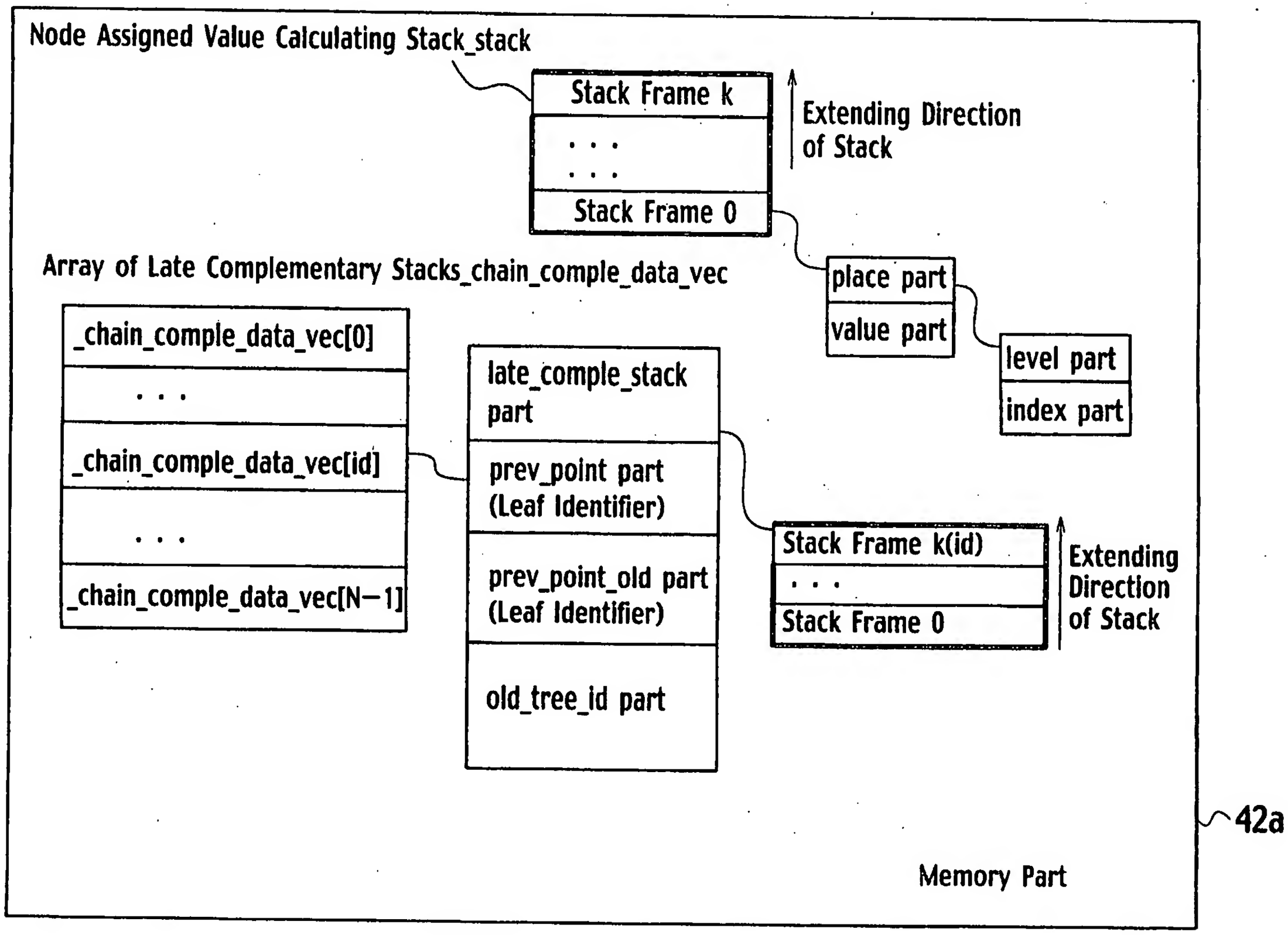

Node Assigned Value Calculating Stack_stack
Stack Frame k
Stack Frame 0
Extending Direction of Stack
Array of Late Complementary Stacks_chain_comple_data_vec
place part
value part
level part
index part
_chain_comple_data_vec[0]
_chain_comple_data_vec[id]
_chain_comple_data_vec[N−1]
late_comple_stack part
prev_point part (Leaf Identifier)
prev_point_old part (Leaf Identifier)
old_tree_id part
Stack Frame k(id)
Stack Frame 0
Extending Direction of Stack
42a
Memory Part

FIG. 51

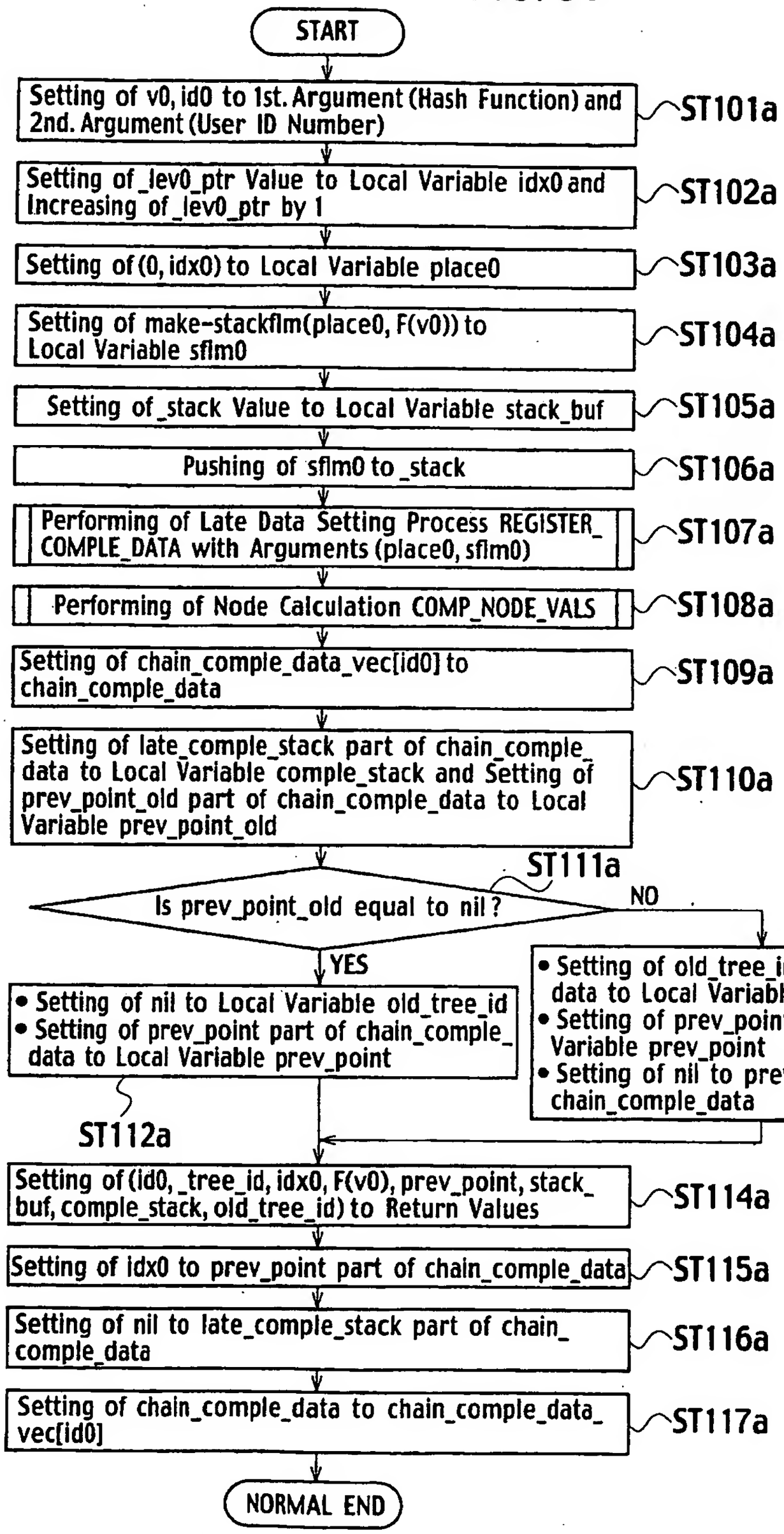

START
Setting of v0, id0 to 1st. Argument (Hash Function) and 2nd. Argument (User ID Number)
ST101a
Setting of _lev0_ptr Value to Local Variable idx0 and Increasing of _lev0_ptr by 1
ST102a
Setting of (0, idx0) to Local Variable place0
ST103a
Setting of make-stackflm(place0, F(v0)) to Local Variable sflm0
ST104a
Setting of _stack Value to Local Variable stack_buf
ST105a
Pushing of sflm0 to _stack
ST106a
Performing of Late Data Setting Process REGISTER_COMPLE_DATA with Arguments (place0, sflm0)
ST107a
Performing of Node Calculation COMP_NODE_VALS
ST108a
Setting of chain_comple_data_vec[id0] to chain_comple_data
ST109a
Setting of late_comple_stack part of chain_comple_data to Local Variable comple_stack and Setting of prev_point_old part of chain_comple_data to Local Variable prev_point_old
ST110a
ST111a
Is prev_point_old equal to nil ?
NO
YES
ST113a
• Setting of nil to Local Variable old_tree_id
• Setting of prev_point part of chain_comple_data to Local Variable prev_point
• Setting of old_tree_id part of chain_comple_data to Local Variable old_tree_id
• Setting of prev_point_old part to Local Variable prev_point
• Setting of nil to prev_point_old part of chain_comple_data
ST112a
Setting of (id0, _tree_id, idx0, F(v0), prev_point, stack_buf, comple_stack, old_tree_id) to Return Values
ST114a
Setting of idx0 to prev_point part of chain_comple_data
ST115a
Setting of nil to late_comple_stack part of chain_comple_data
ST116a
Setting of chain_comple_data to chain_comple_data_vec[id0]
ST117a
NORMAL END

FIG. 52

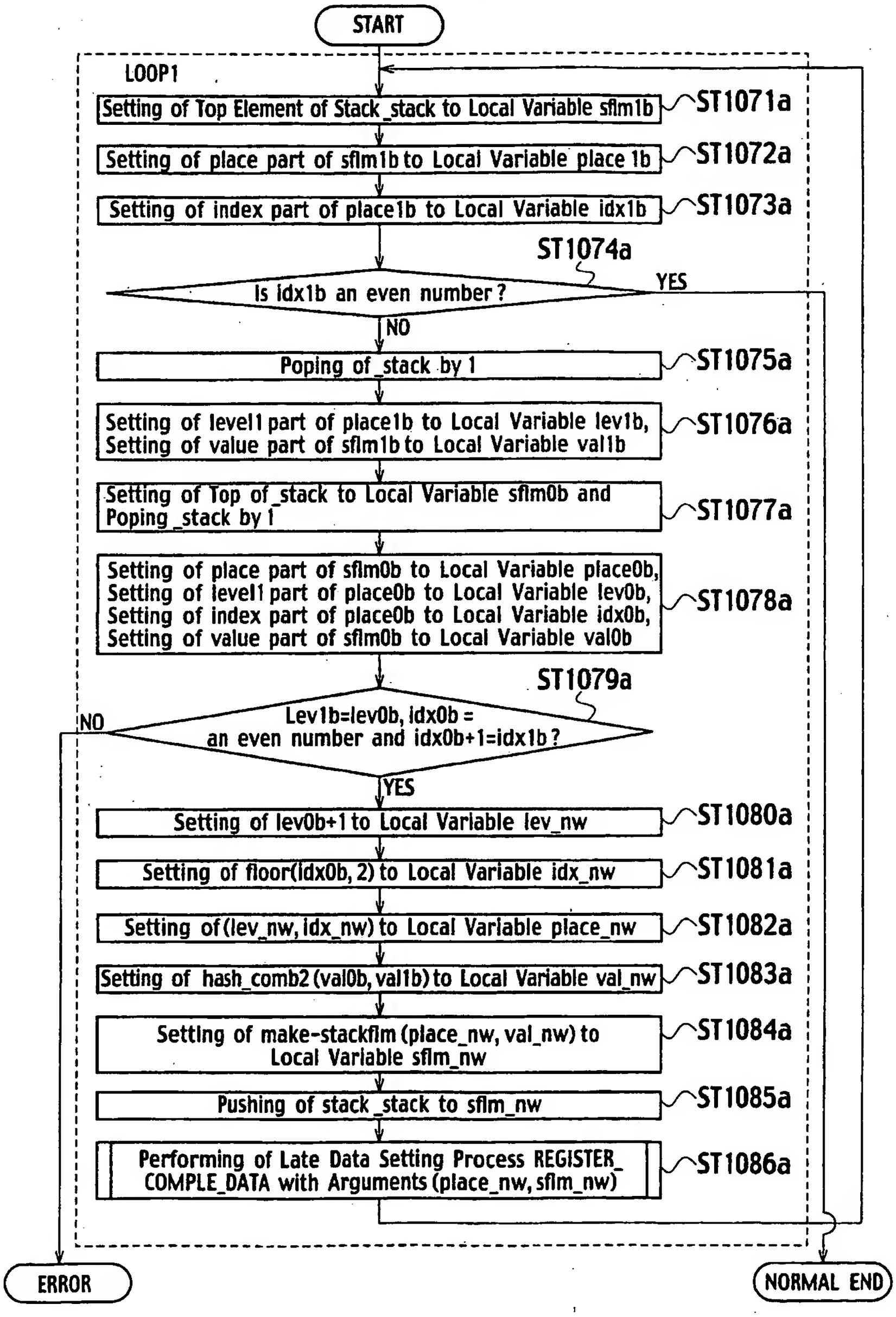

START
LOOP1
Setting of Top Element of Stack_stack to Local Variable sflm1b
ST1071a
Setting of place part of sflm1b to Local Variable place1b
ST1072a
Setting of index part of place1b to Local Variable idx1b
ST1073a
ST1074a
Is idx1b an even number?
YES
NO
Poping of_stack by 1
ST1075a
Setting of level1 part of place1b to Local Variable lev1b,
Setting of value part of sflm1b to Local Variable val1b
ST1076a
Setting of Top of_stack to Local Variable sflm0b and
Poping_stack by 1
ST1077a
Setting of place part of sflm0b to Local Variable place0b,
Setting of level1 part of place0b to Local Variable lev0b,
Setting of index part of place0b to Local Variable idx0b,
Setting of value part of sflm0b to Local Variable val0b
ST1078a
ST1079a
Lev1b=lev0b, idx0b =
an even number and idx0b+1=idx1b?
NO
YES
Setting of lev0b+1 to Local Variable lev_nw
ST1080a
Setting of floor(idx0b, 2) to Local Variable idx_nw
ST1081a
Setting of(lev_nw, idx_nw) to Local Variable place_nw
ST1082a
Setting of hash_comb2(val0b, val1b) to Local Variable val_nw
ST1083a
Setting of make-stackflm(place_nw, val_nw) to
Local Variable sflm_nw
ST1084a
Pushing of stack_stack to sflm_nw
ST1085a
Performing of Late Data Setting Process REGISTER_
COMPLE_DATA with Arguments(place_nw, sflm_nw)
ST1086a
ERROR
NORMAL END

FIG. 53

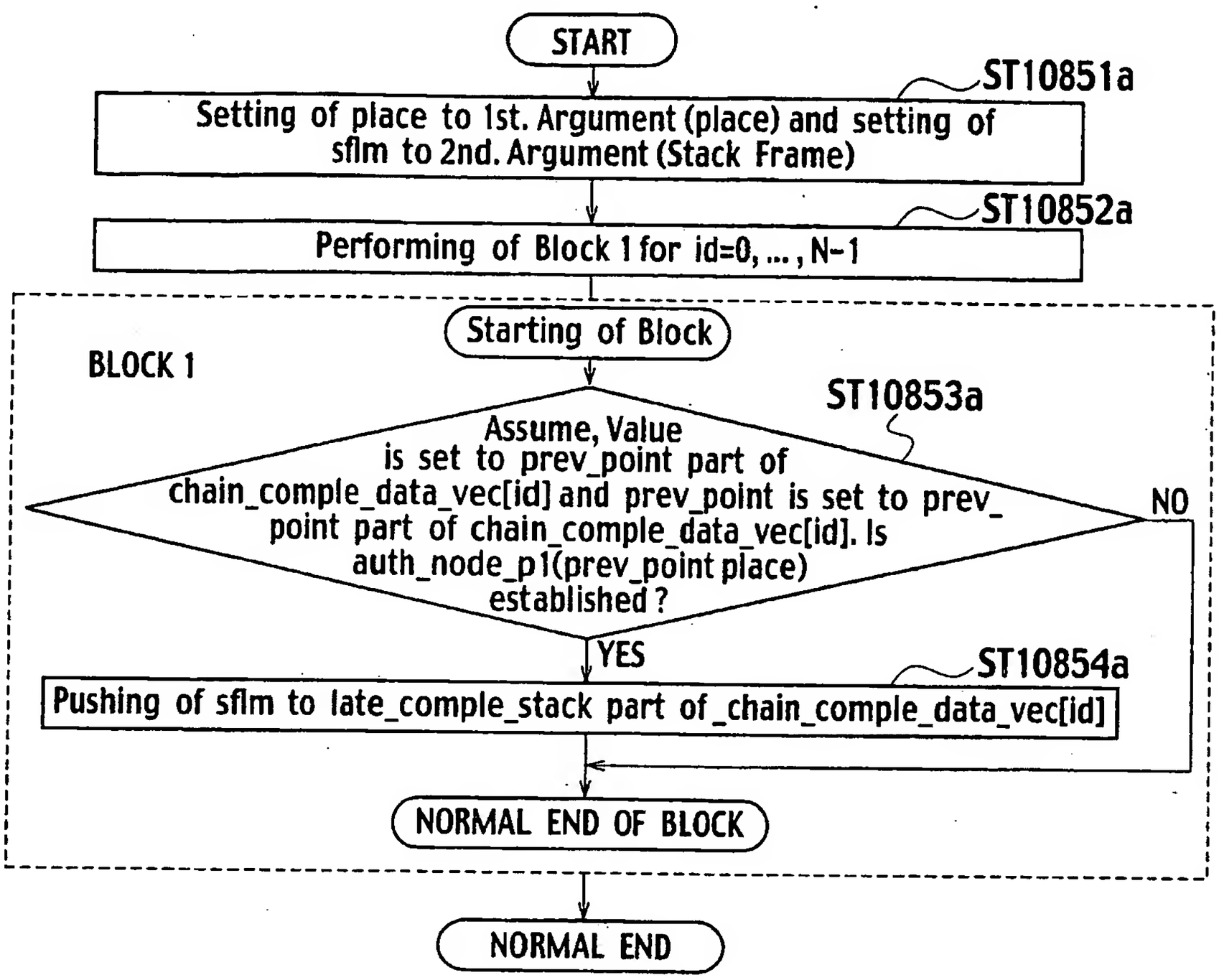

START
Setting of place to 1st. Argument (place) and setting of sflm to 2nd. Argument (Stack Frame)
ST10851a
Performing of Block 1 for id=0, ... , N-1
ST10852a
BLOCK 1
Starting of Block
Assume, Value is set to prev_point part of chain_comple_data_vec[id] and prev_point is set to prev_point part of chain_comple_data_vec[id]. Is auth_node_p1(prev_point place) established ?
ST10853a
NO
YES
Pushing of sflm to late_comple_stack part of_chain_comple_data_vec[id]
ST10854a
NORMAL END OF BLOCK
NORMAL END

FIG. 54

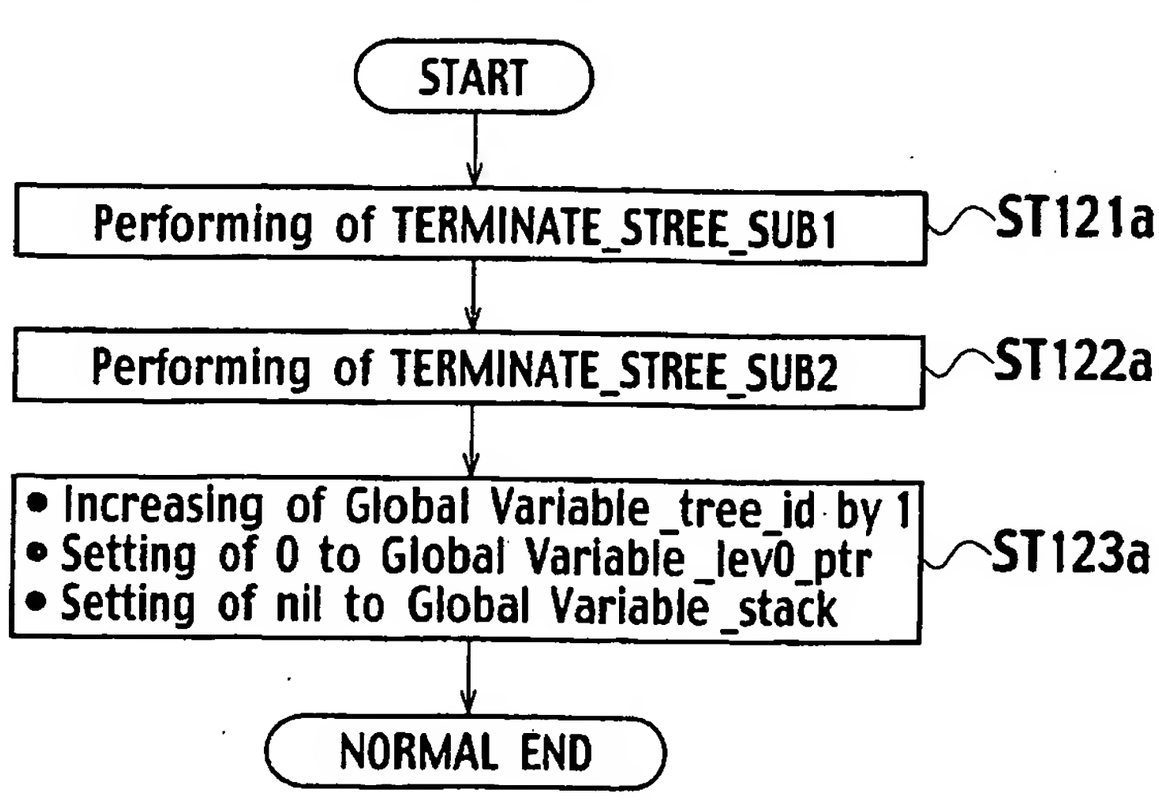

START
Performing of TERMINATE_STREE_SUB1
ST121a
Performing of TERMINATE_STREE_SUB2
ST122a
• Increasing of Global Variable _tree_id by 1
• Setting of 0 to Global Variable _lev0_ptr
• Setting of nil to Global Variable _stack
ST123a
NORMAL END

FIG. 55

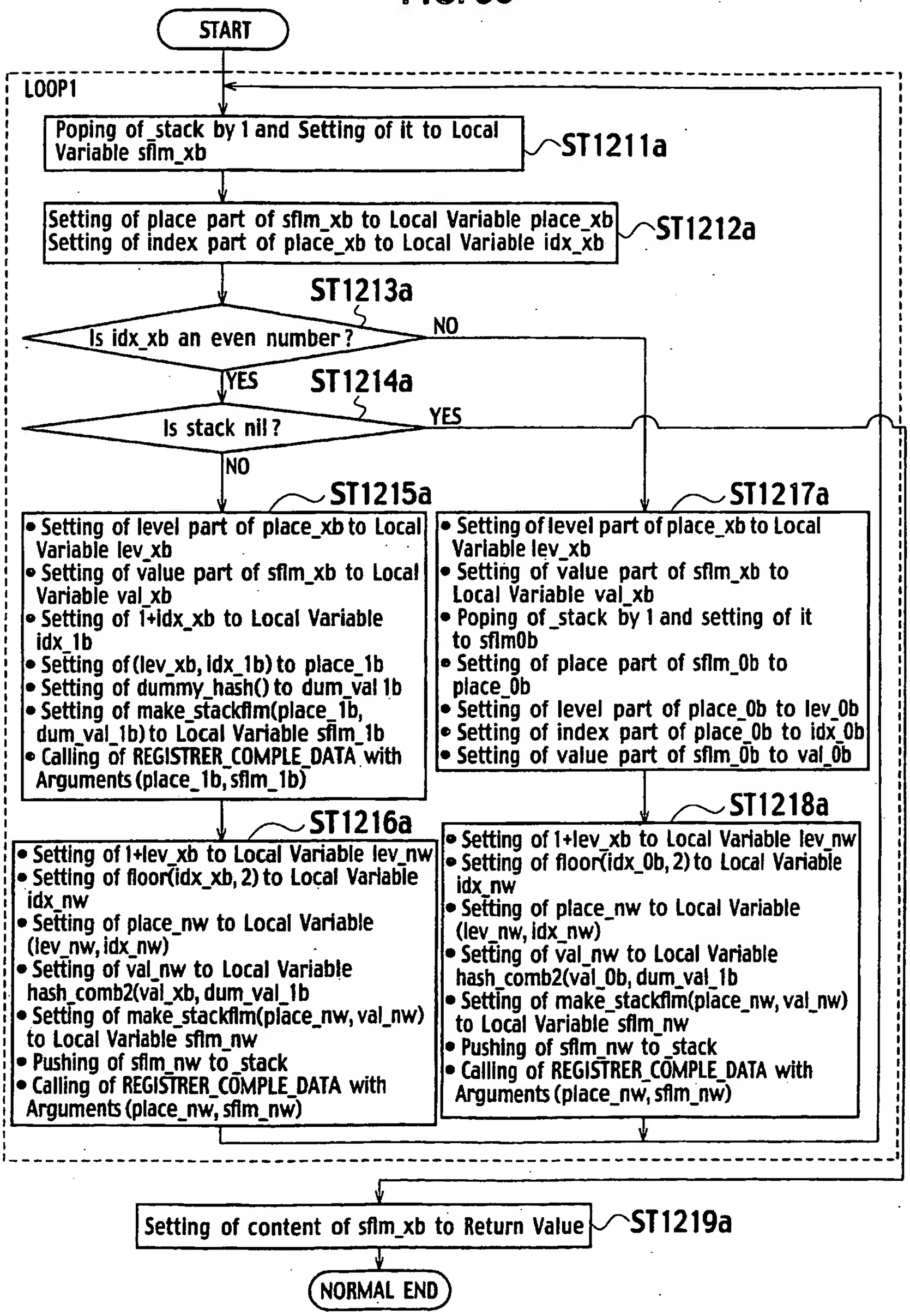

START
LOOP1
Poping of_stack by 1 and Setting of it to Local Variable sfim_xb
ST1211a
Setting of place part of sfim_xb to Local Variable place_xb
Setting of index part of place_xb to Local Variable idx_xb
ST1212a
ST1213a
Is idx_xb an even number?
NO
YES
ST1214a
Is stack nil?
YES
NO
ST1215a
• Setting of level part of place_xb to Local Variable lev_xb
• Setting of value part of sfim_xb to Local Variable val_xb
• Setting of 1+idx_xb to Local Variable idx_1b
• Setting of (lev_xb, idx_1b) to place_1b
• Setting of dummy_hash() to dum_val 1b
• Setting of make_stackfim(place_1b, dum_val_1b) to Local Variable sfim_1b
• Calling of REGISTRER_COMPLE_DATA with Arguments (place_1b, sfim_1b)
ST1216a
• Setting of 1+lev_xb to Local Variable lev_nw
• Setting of floor(idx_xb, 2) to Local Variable idx_nw
• Setting of place_nw to Local Variable (lev_nw, idx_nw)
• Setting of val_nw to Local Variable hash_comb2(val_xb, dum_val_1b
• Setting of make_stackfim(place_nw, val_nw) to Local Variable sfim_nw
• Pushing of sfim_nw to _stack
• Calling of REGISTRER_COMPLE_DATA with Arguments (place_nw, sfim_nw)
ST1217a
• Setting of level part of place_xb to Local Variable lev_xb
• Setting of value part of sfim_xb to Local Variable val_xb
• Poping of _stack by 1 and setting of it to sfim0b
• Setting of place part of sfim_0b to place_0b
• Setting of level part of place_0b to lev_0b
• Setting of index part of place_0b to idx_0b
• Setting of value part of sfim_0b to val_0b
ST1218a
• Setting of 1+lev_xb to Local Variable lev_nw
• Setting of floor(idx_0b, 2) to Local Variable idx_nw
• Setting of place_nw to Local Variable (lev_nw, idx_nw)
• Setting of val_nw to Local Variable hash_comb2(val_0b, dum_val_1b
• Setting of make_stackfim(place_nw, val_nw) to Local Variable sfim_nw
• Pushing of sfim_nw to _stack
• Calling of REGISTRER_COMPLE_DATA with Arguments (place_nw, sfim_nw)
Setting of content of sfim_xb to Return Value
ST1219a
NORMAL END

FIG. 56

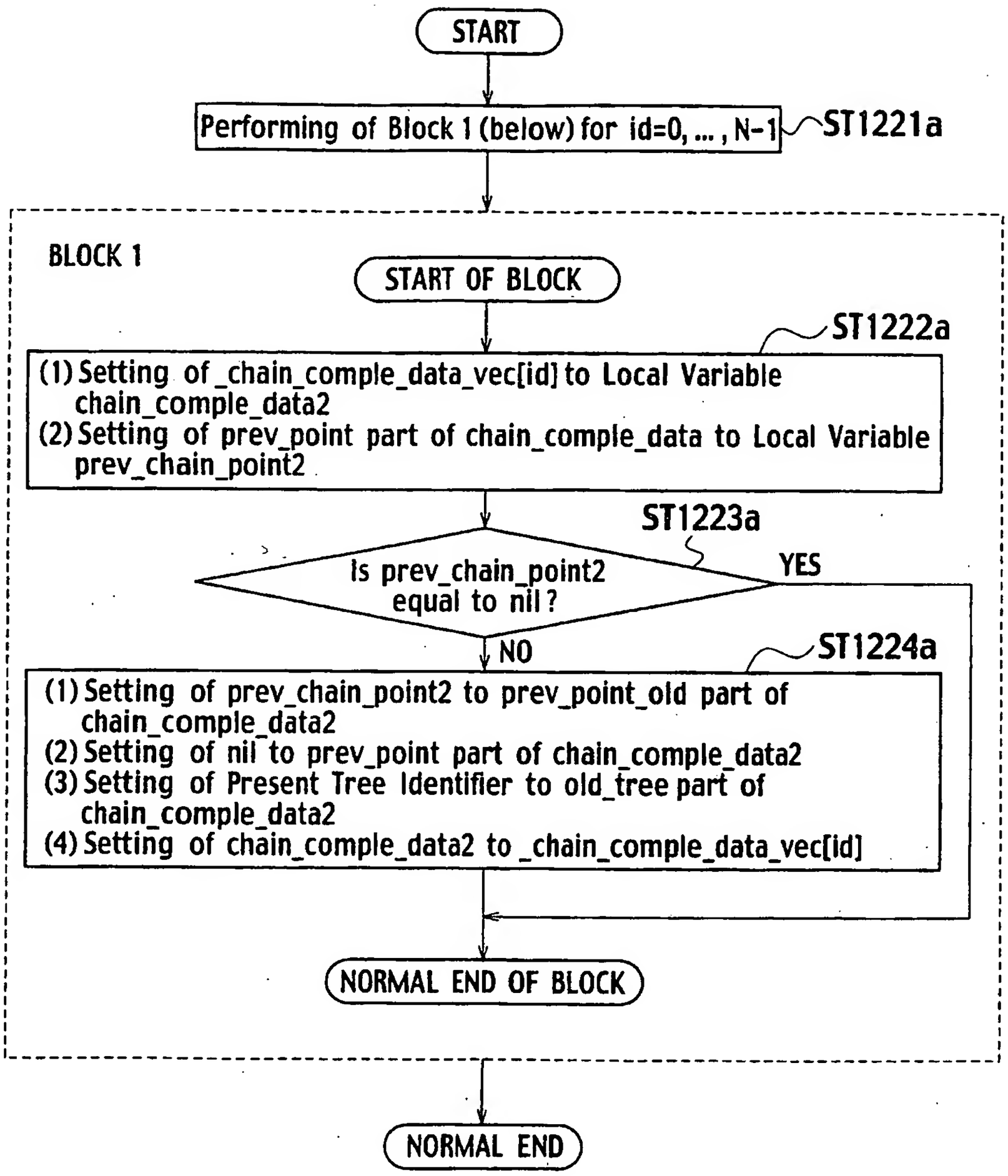
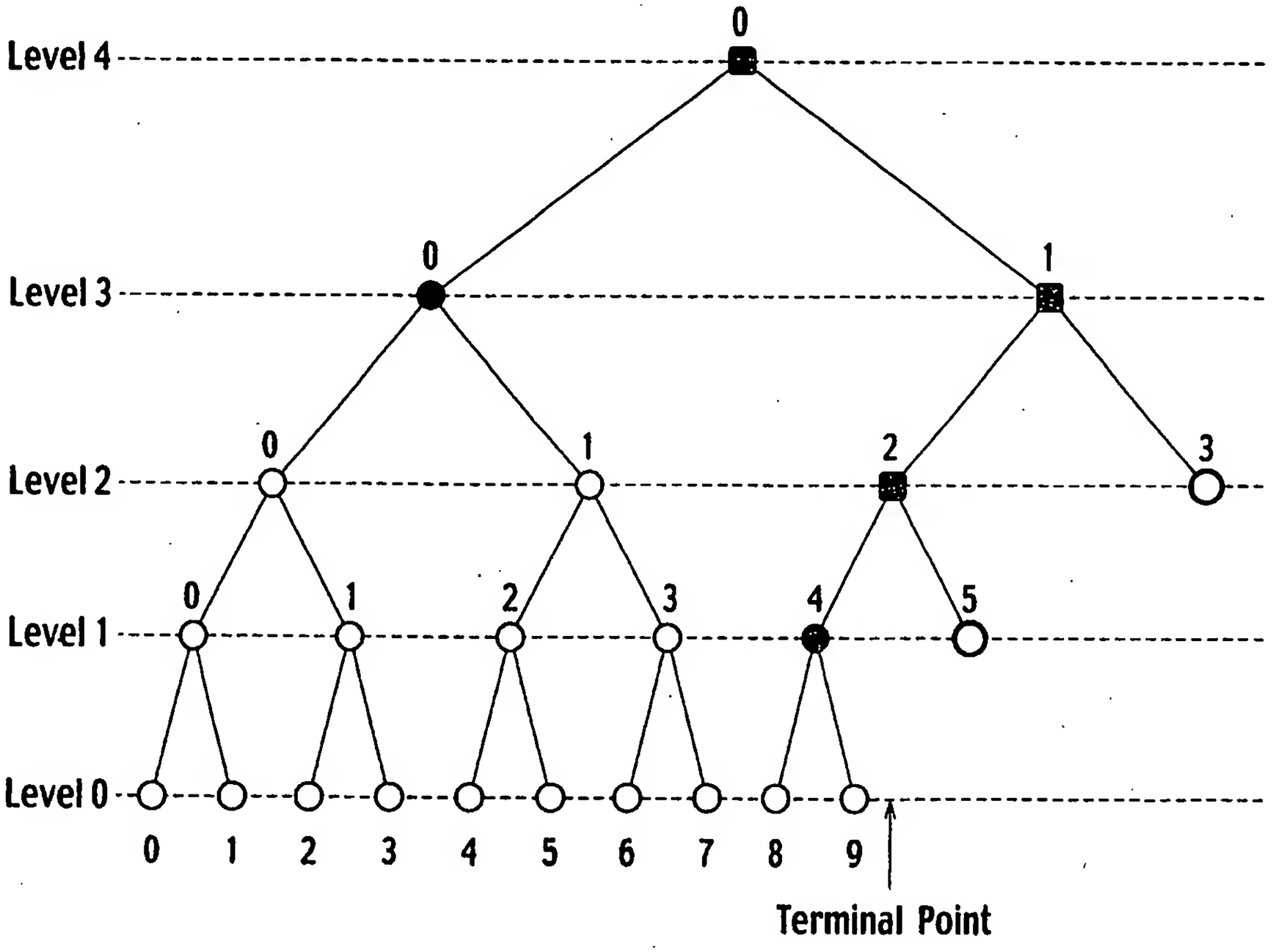

START
Performing of Block 1 (below) for id=0, ... , N-1
ST1221a
BLOCK 1
START OF BLOCK
ST1222a
(1) Setting of _chain_comple_data_vec[id] to Local Variable chain_comple_data2
(2) Setting of prev_point part of chain_comple_data to Local Variable prev_chain_point2
ST1223a
Is prev_chain_point2 equal to nil?
YES
NO
ST1224a
(1) Setting of prev_chain_point2 to prev_point_old part of chain_comple_data2
(2) Setting of nil to prev_point part of chain_comple_data2
(3) Setting of Present Tree Identifier to old_tree part of chain_comple_data2
(4) Setting of chain_comple_data2 to _chain_comple_data_vec[id]
NORMAL END OF BLOCK
NORMAL END

FIG. 57


Level 4
Level 3
Level 2
Level 1
Level 0
0
0
1
0
1
2
3
0
1
2
3
4
5
0 1 2 3 4 5 6 7 8 9
Terminal Point

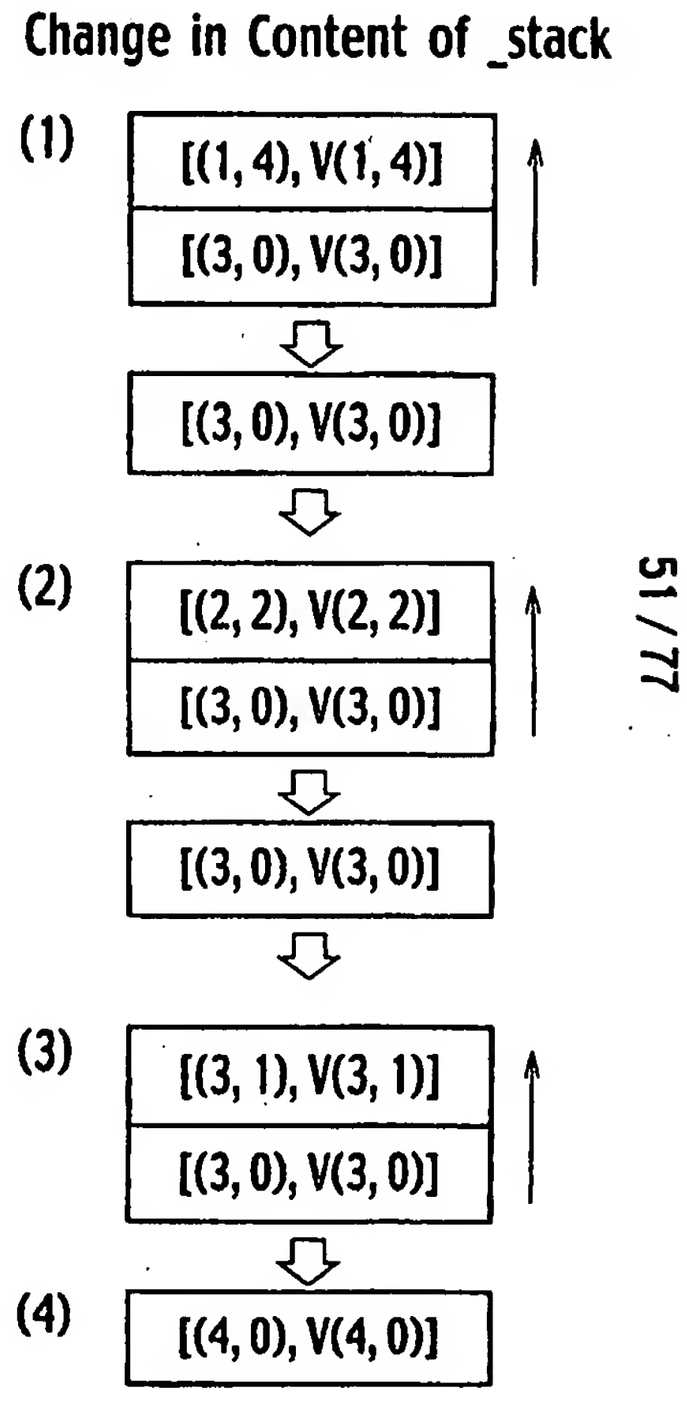

Change in Content of _stack
(1)
[(1, 4), V(1, 4)]
[(3, 0), V(3, 0)]
[(3, 0), V(3, 0)]
(2)
[(2, 2), V(2, 2)]
[(3, 0), V(3, 0)]
[(3, 0), V(3, 0)]
(3)
[(3, 1), V(3, 1)]
[(3, 0), V(3, 0)]
(4)
[(4, 0), V(4, 0)]

FIG. 58

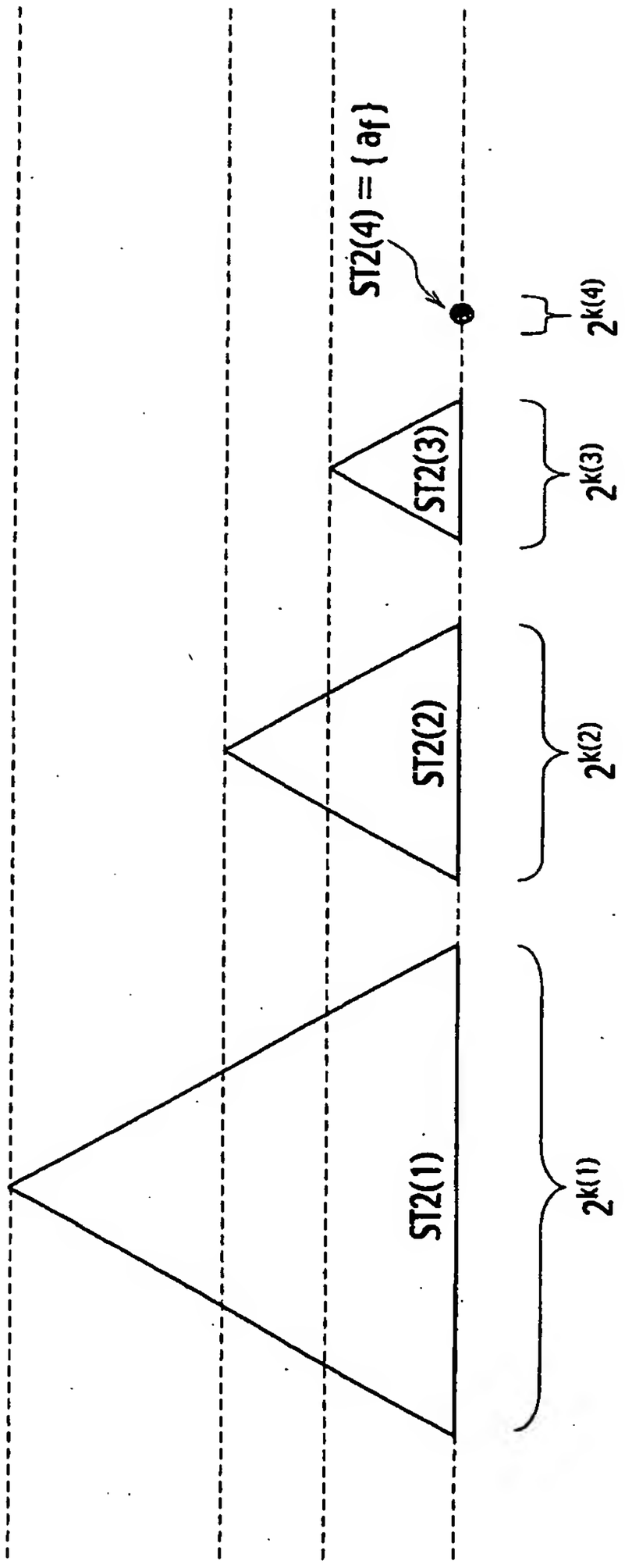


FIG. 59

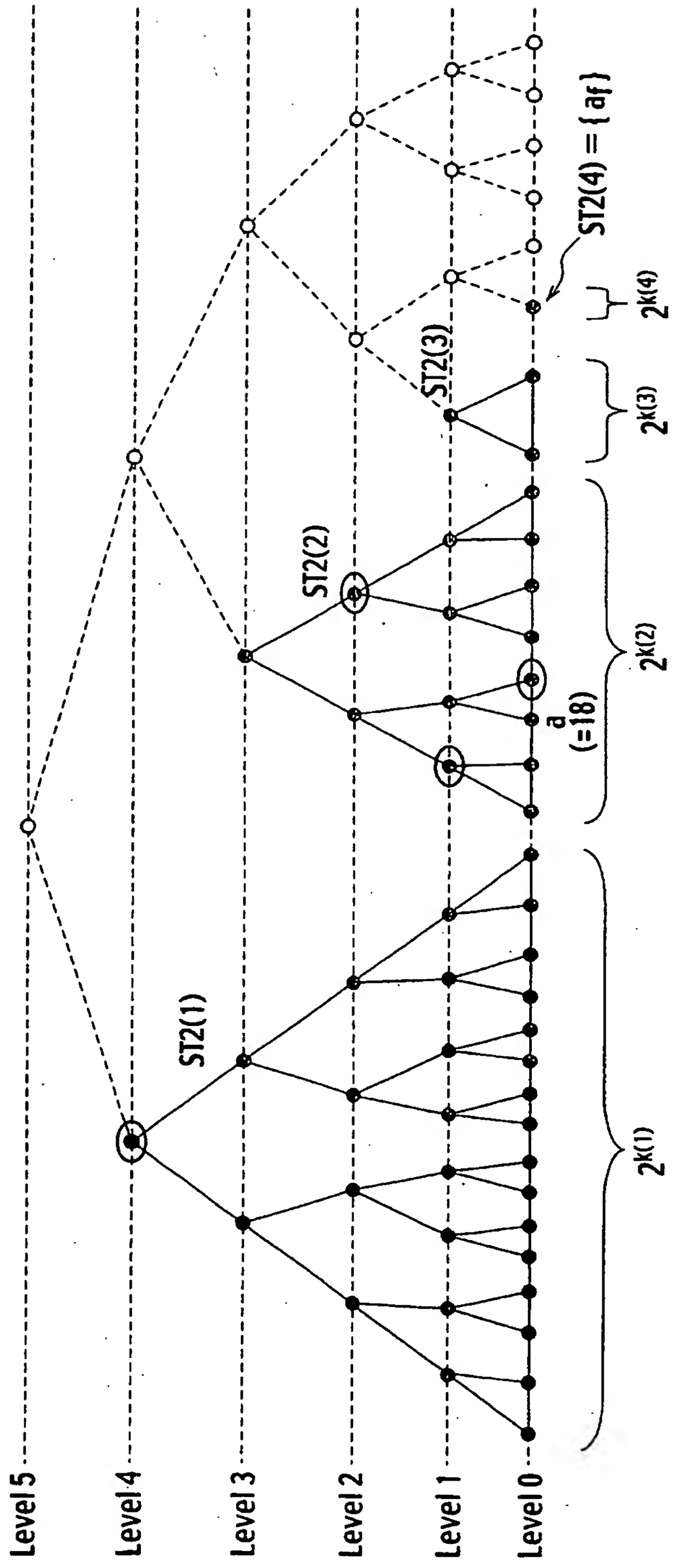

Level 5
Level 4
Level 3
Level 2
Level 1
Level 0
ST2(1)
ST2(2)
ST2(3)
ST2(4) = {af}
a
(=18)
$2^{k(1)}$
$2^{k(2)}$
$2^{k(3)}$
$2^{k(4)}$
k(1)=4 >k(2)=3 >k(3)=1 >k(4) = 0

FIG. 60

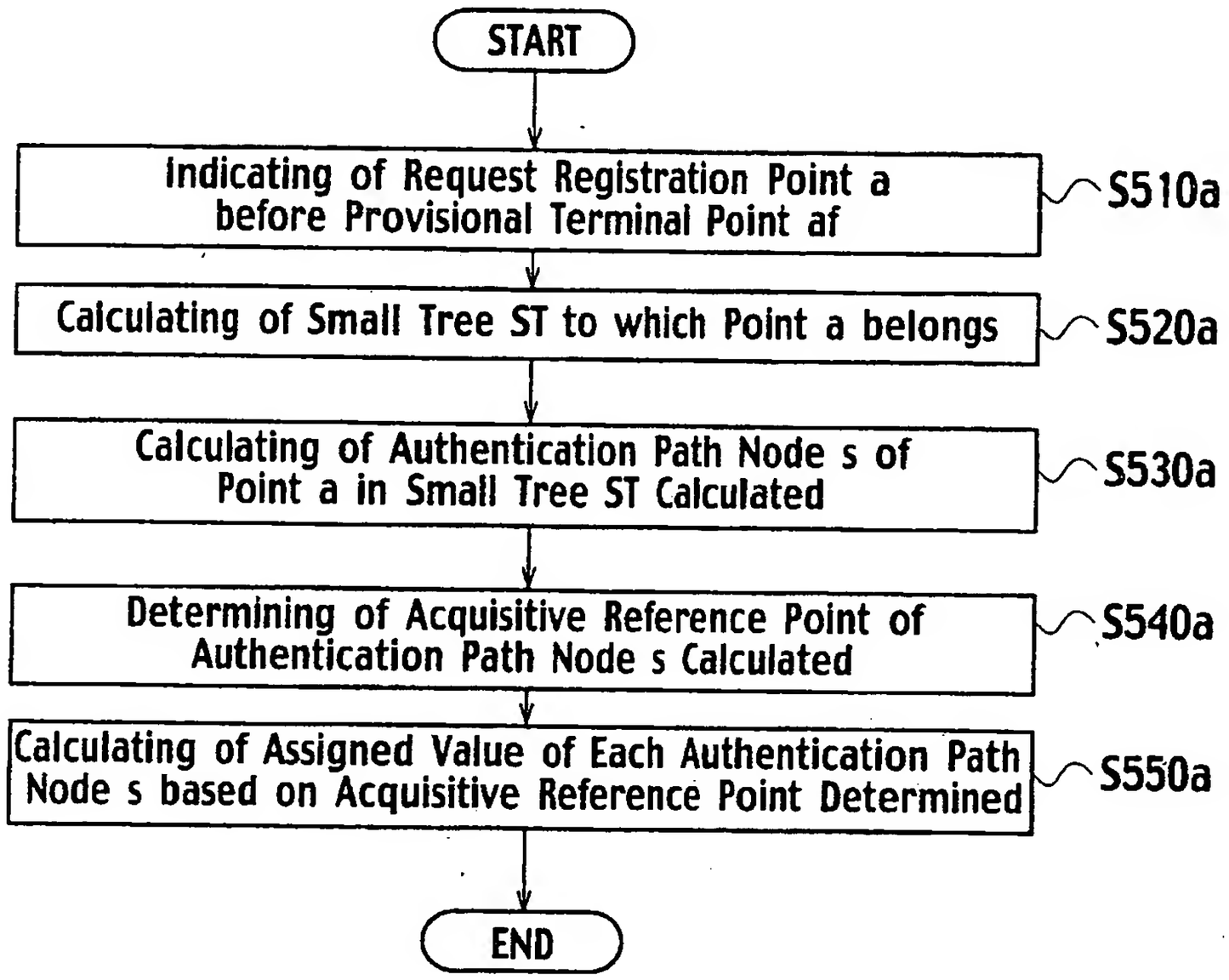
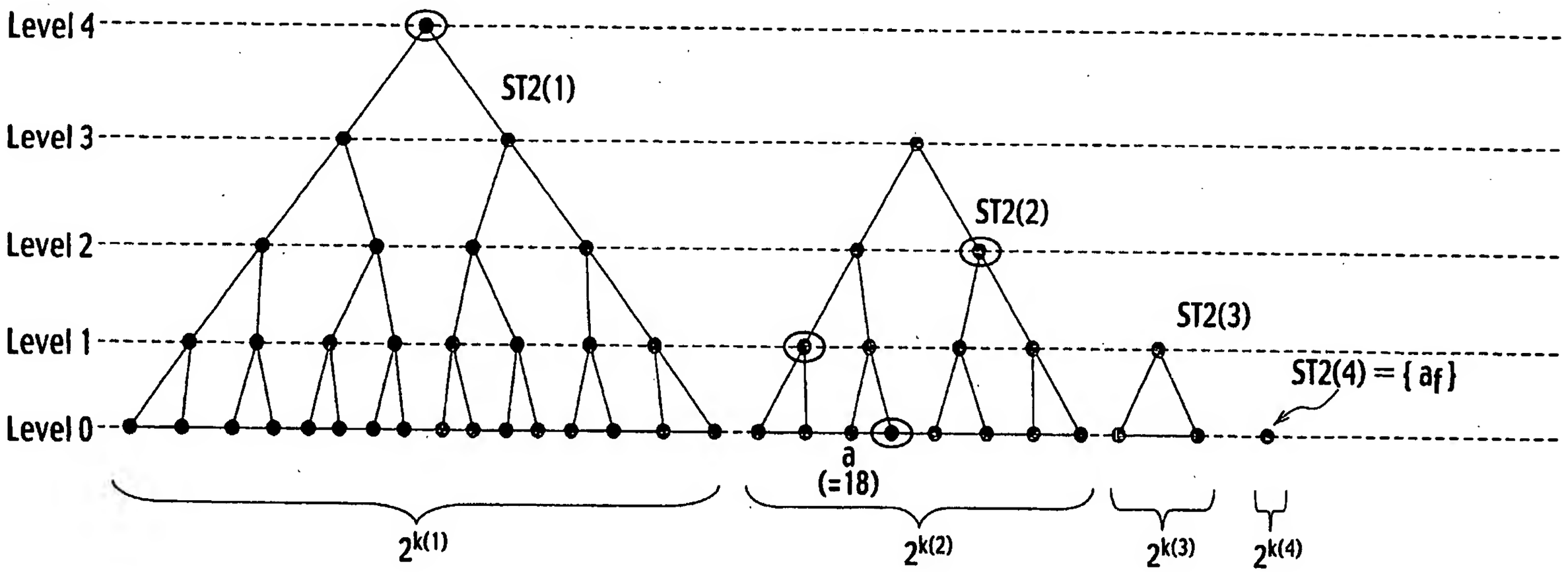

START
Indicating of Request Registration Point a before Provisional Terminal Point af
S510a
Calculating of Small Tree ST to which Point a belongs
S520a
Calculating of Authentication Path Node s of Point a in Small Tree ST Calculated
S530a
Determining of Acquisitive Reference Point of Authentication Path Node s Calculated
S540a
Calculating of Assigned Value of Each Authentication Path Node s based on Acquisitive Reference Point Determined
S550a
END

FIG. 61



k(1)=4 >k(2)=3 >k(3)=1 >k(4)=0

FIG. 62

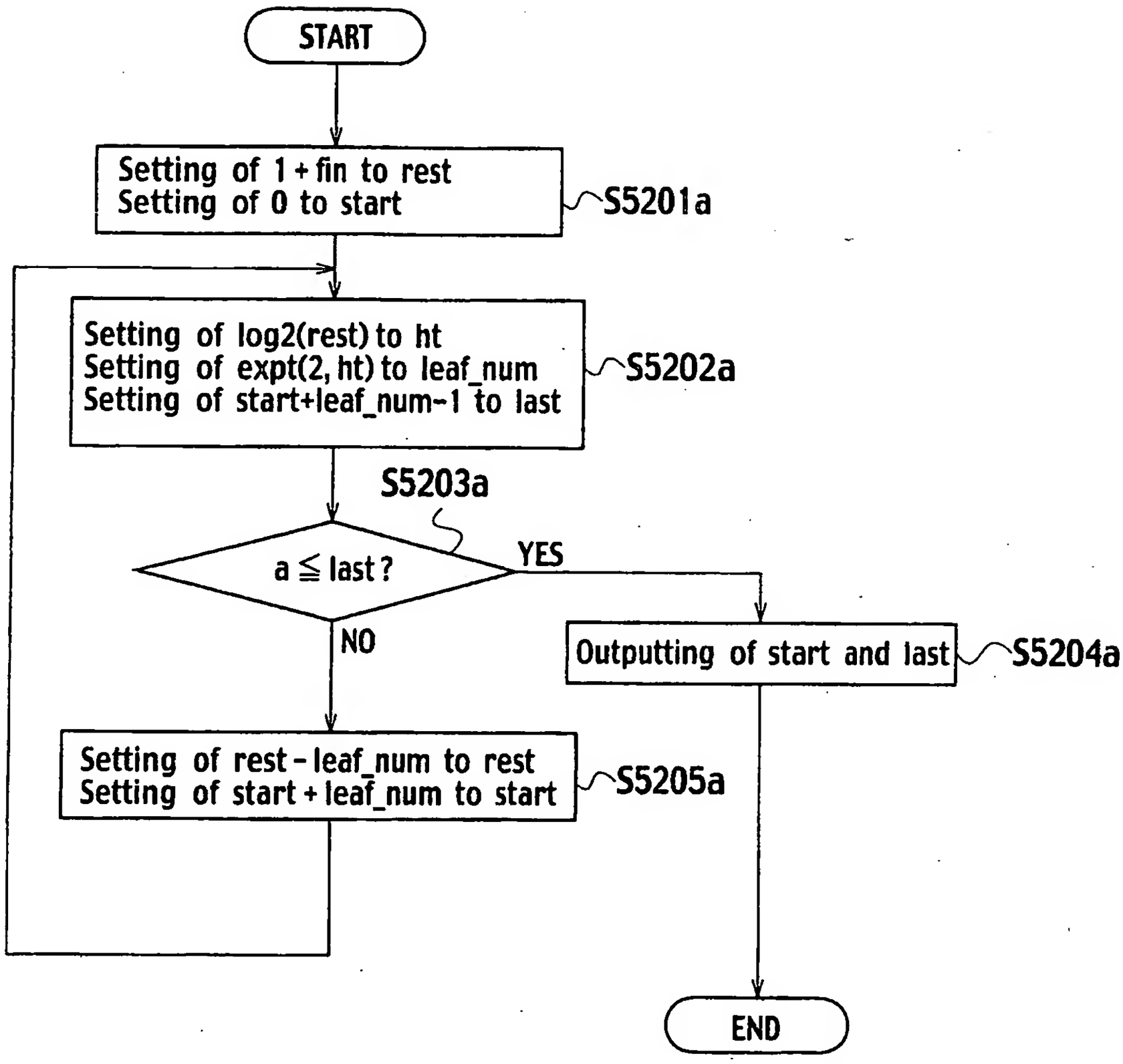

START
Setting of 1 + fin to rest
Setting of 0 to start
S5201a
Setting of log2(rest) to ht
Setting of expt(2, ht) to leaf_num
Setting of start+leaf_num-1 to last
S5202a
S5203a
a ≦ last ?
YES
NO
Outputting of start and last
S5204a
Setting of rest - leaf_num to rest
Setting of start + leaf_num to start
S5205a
END

FIG. 63

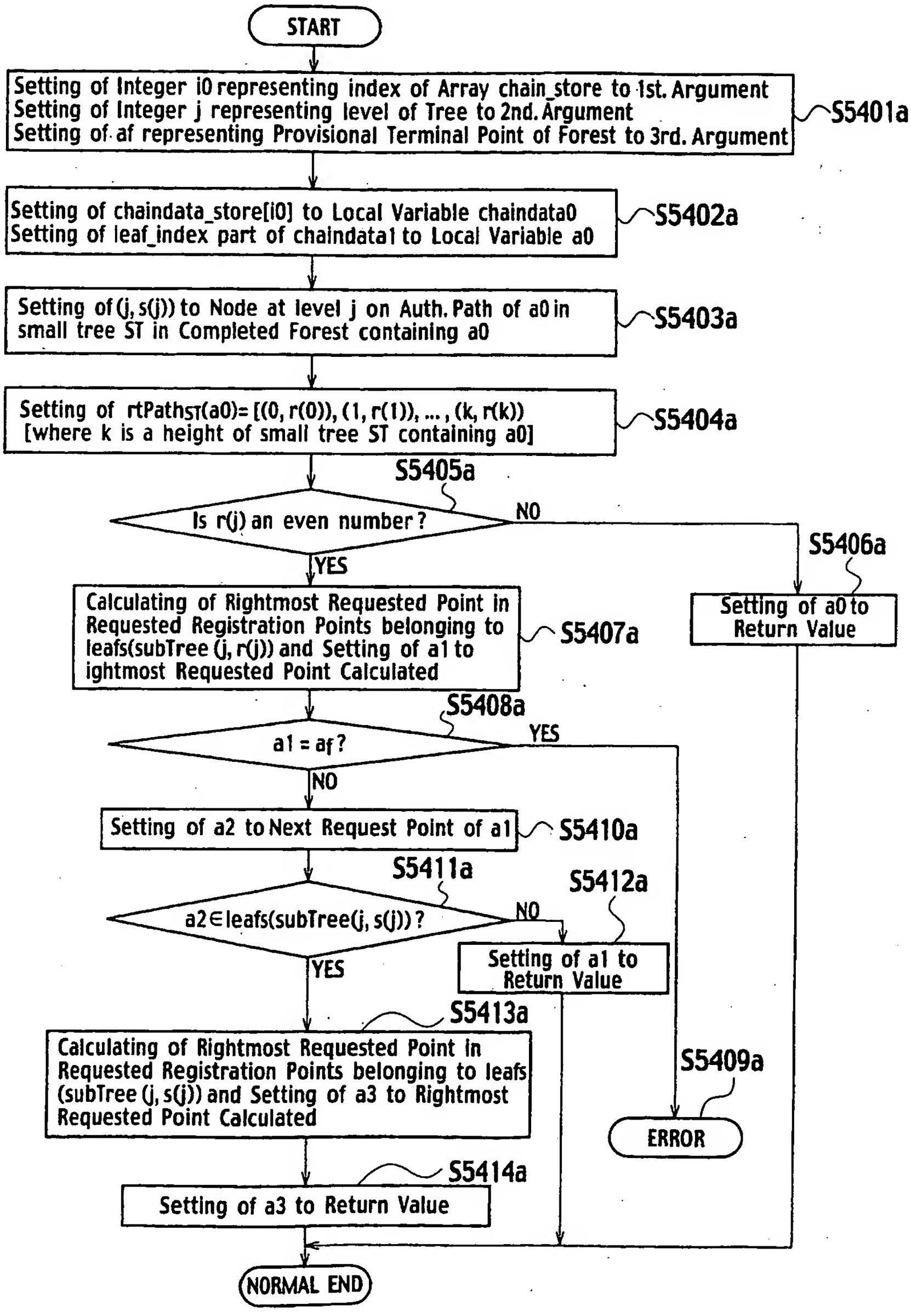

START
Setting of Integer i0 representing index of Array chain_store to 1st. Argument
Setting of Integer j representing level of Tree to 2nd. Argument
Setting of af representing Provisional Terminal Point of Forest to 3rd. Argument
S5401a
Setting of chaindata_store[i0] to Local Variable chaindata0
Setting of leaf_index part of chaindata1 to Local Variable a0
S5402a
Setting of (j, s(j)) to Node at level j on Auth. Path of a0 in small tree ST in Completed Forest containing a0
S5403a
Setting of rtPathsT(a0)= [(0, r(0)), (1, r(1)), ... , (k, r(k))
[where k is a height of small tree ST containing a0]
S5404a
S5405a
Is r(j) an even number?
NO
YES
S5406a
Setting of a0 to Return Value
Calculating of Rightmost Requested Point in Requested Registration Points belonging to leafs(subTree (j, r(j)) and Setting of a1 to ightmost Requested Point Calculated
S5407a
S5408a
a1 = af?
YES
NO
Setting of a2 to Next Request Point of a1
S5410a
S5411a
a2∈leafs(subTree(j, s(j))?
NO
S5412a
YES
Setting of a1 to Return Value
S5413a
Calculating of Rightmost Requested Point in Requested Registration Points belonging to leafs (subTree (j, s(j)) and Setting of a3 to Rightmost Requested Point Calculated
S5409a
ERROR
S5414a
Setting of a3 to Return Value
NORMAL END

FIG. 64

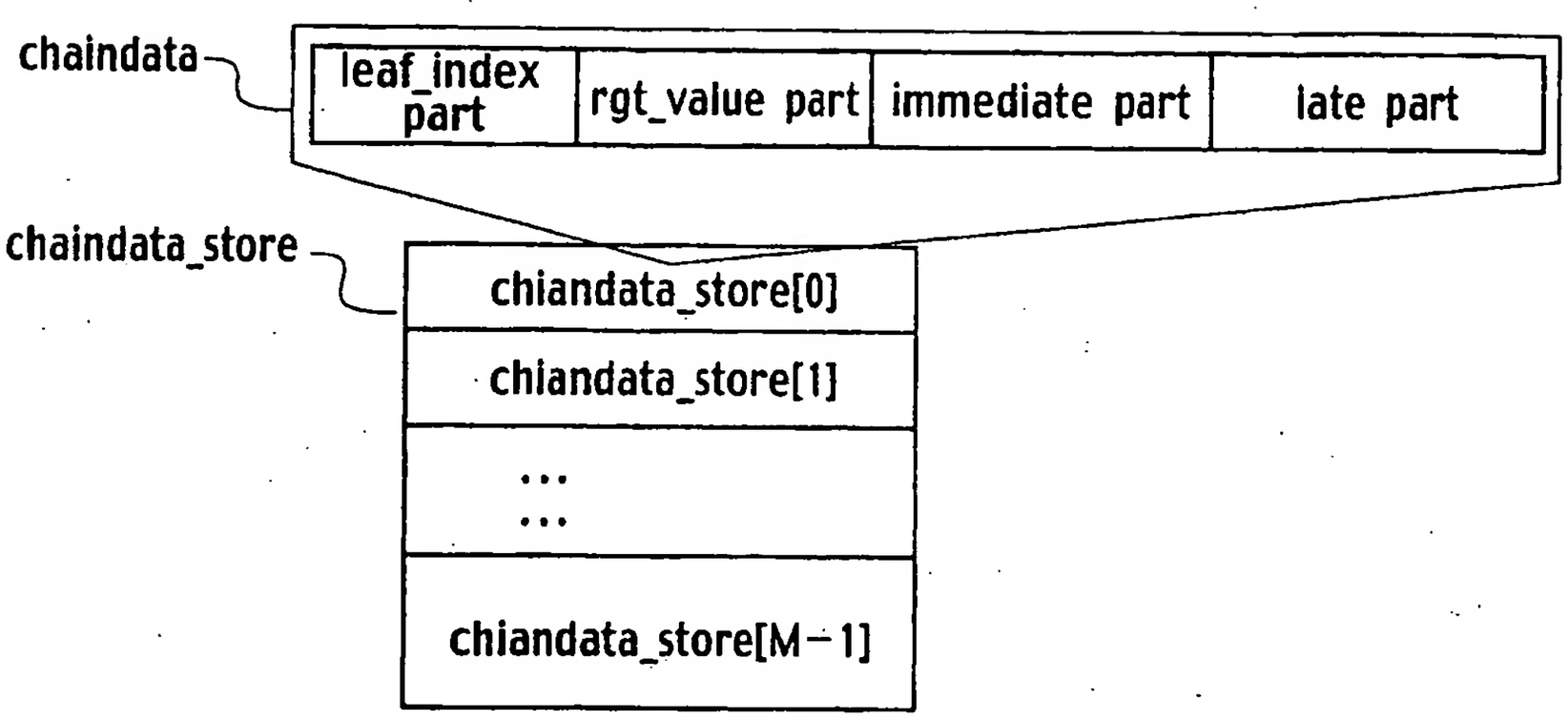

chaindata
leaf_index part
rgt_value part
immediate part
late part
chaindata_store
chiandata_store[0]
chiandata_store[1]
...
chiandata_store[M−1]

FIG. 65A

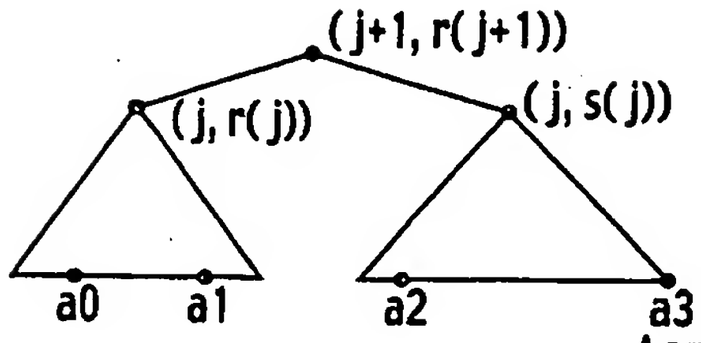


FIG. 65B

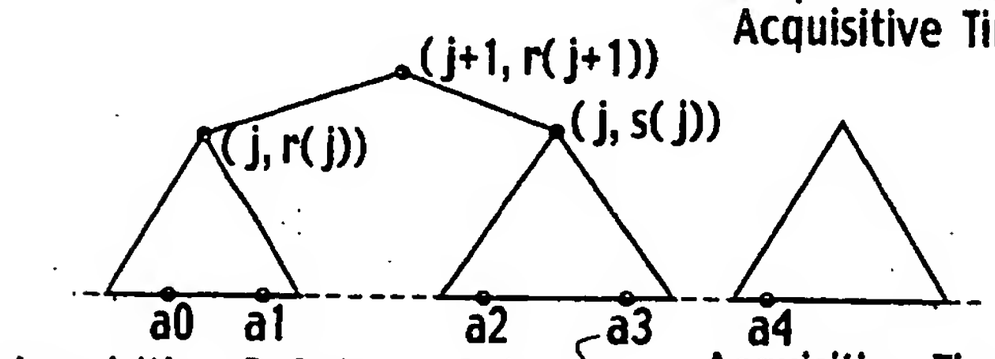


FIG. 65C

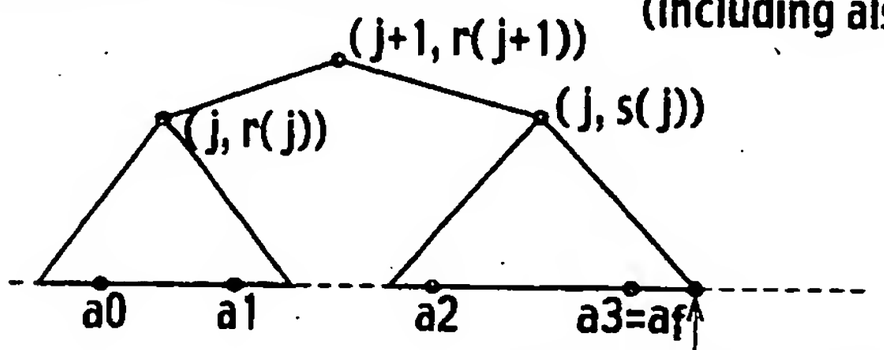


FIG. 65D

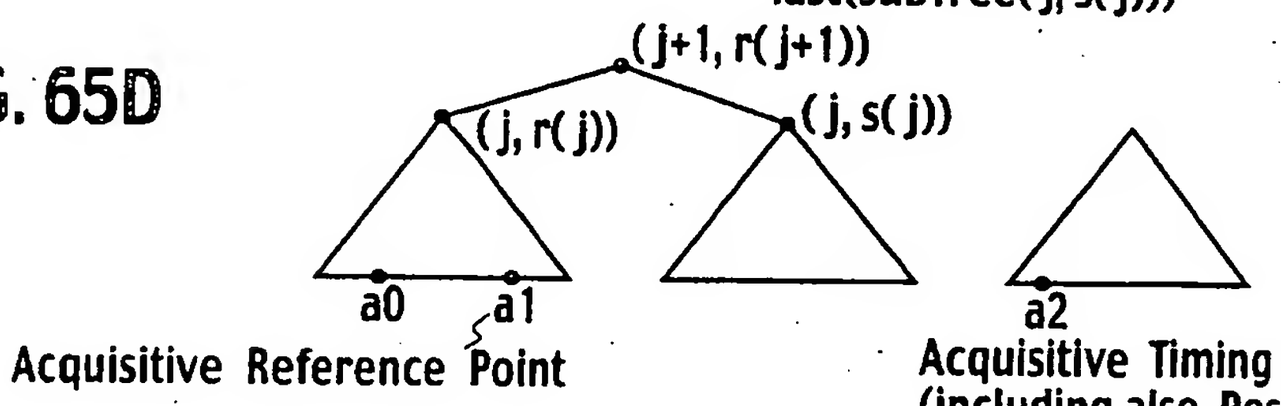


FIG. 65E

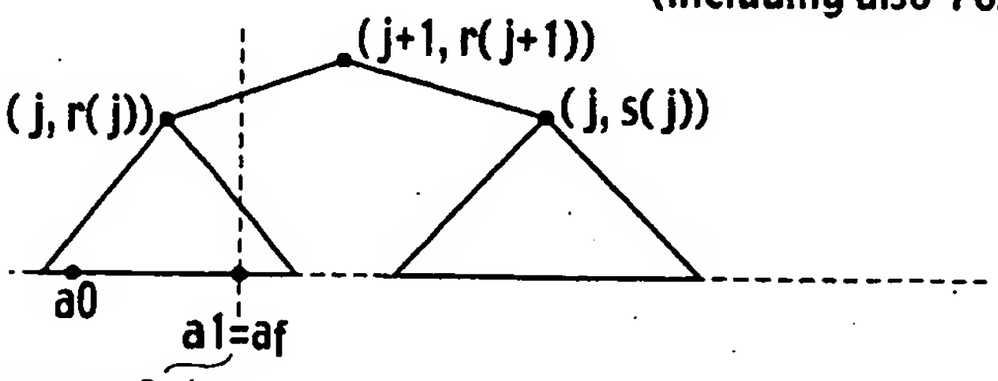


FIG. 65F

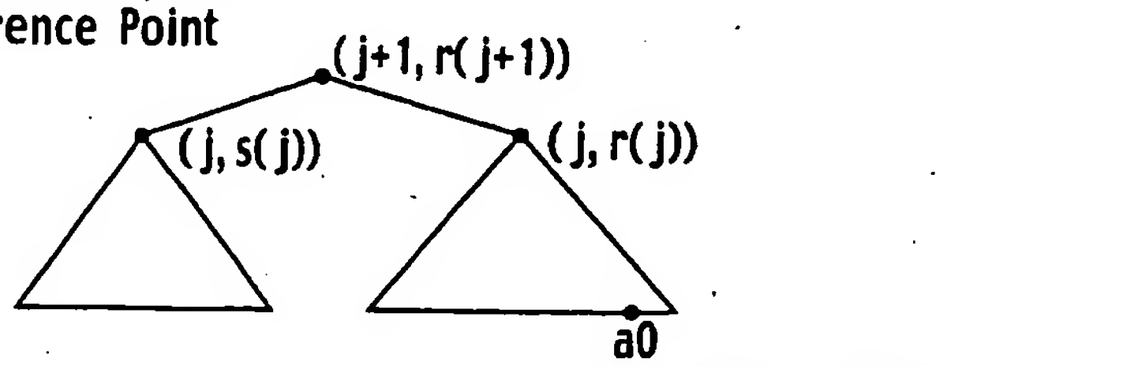


FIG. 66

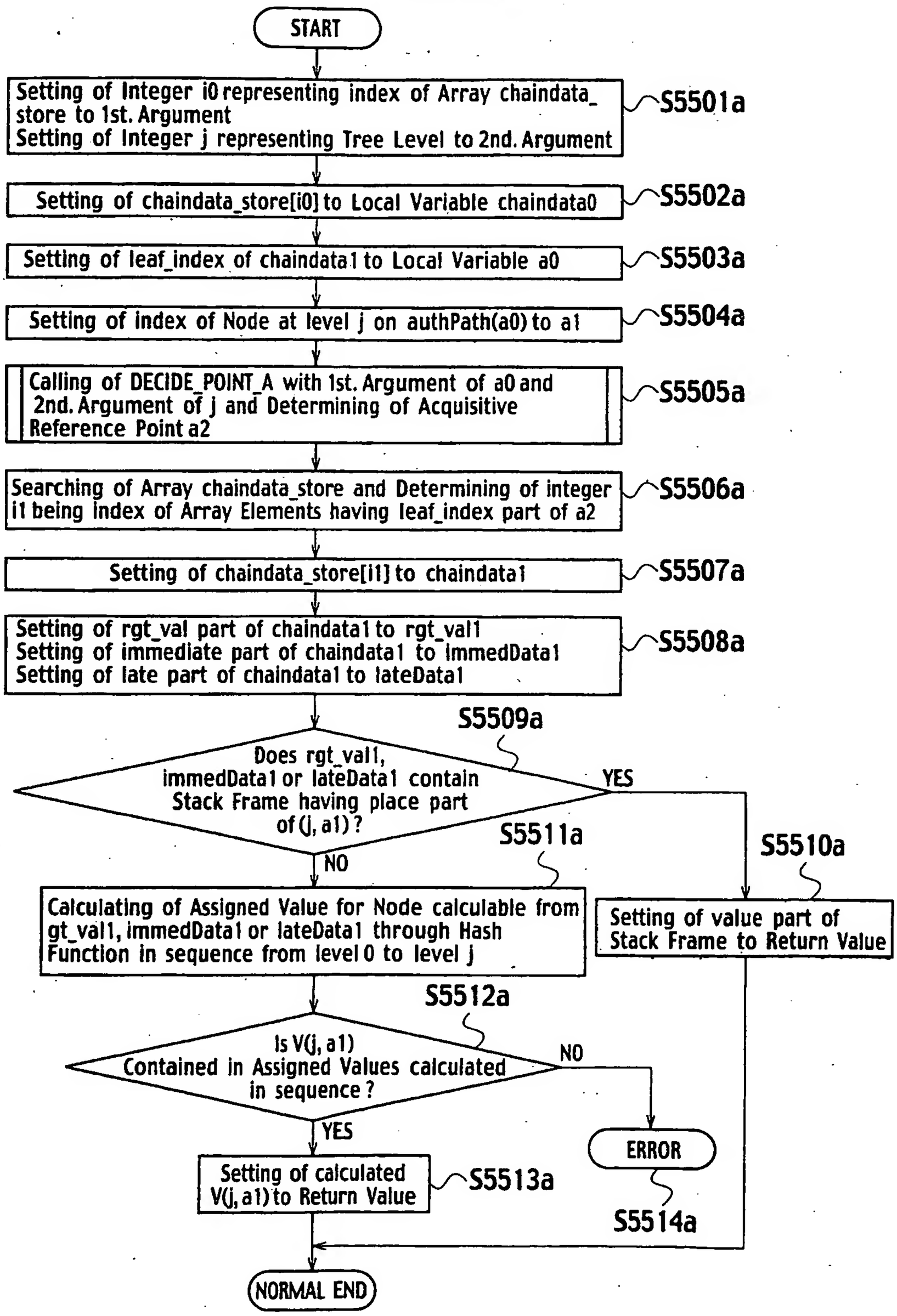

START
Setting of Integer i0 representing index of Array chaindata_store to 1st. Argument
Setting of Integer j representing Tree Level to 2nd. Argument
S5501a
Setting of chaindata_store[i0] to Local Variable chaindata0
S5502a
Setting of leaf_index of chaindata1 to Local Variable a0
S5503a
Setting of index of Node at level j on authPath(a0) to a1
S5504a
Calling of DECIDE_POINT_A with 1st. Argument of a0 and 2nd. Argument of j and Determining of Acquisitive Reference Point a2
S5505a
Searching of Array chaindata_store and Determining of integer i1 being index of Array Elements having leaf_index part of a2
S5506a
Setting of chaindata_store[i1] to chaindata1
S5507a
Setting of rgt_val part of chaindata1 to rgt_val1
Setting of immediate part of chaindata1 to immedData1
Setting of late part of chaindata1 to lateData1
S5508a
S5509a
Does rgt_val1, immedData1 or lateData1 contain Stack Frame having place part of (j, a1)?
YES
NO
S5510a
Setting of value part of Stack Frame to Return Value
S5511a
Calculating of Assigned Value for Node calculable from gt_val1, immedData1 or lateData1 through Hash Function in sequence from level 0 to level j
S5512a
Is V(j, a1) Contained in Assigned Values calculated in sequence?
NO
YES
ERROR
S5514a
Setting of calculated V(j, a1) to Return Value
S5513a
NORMAL END

FIG. 67

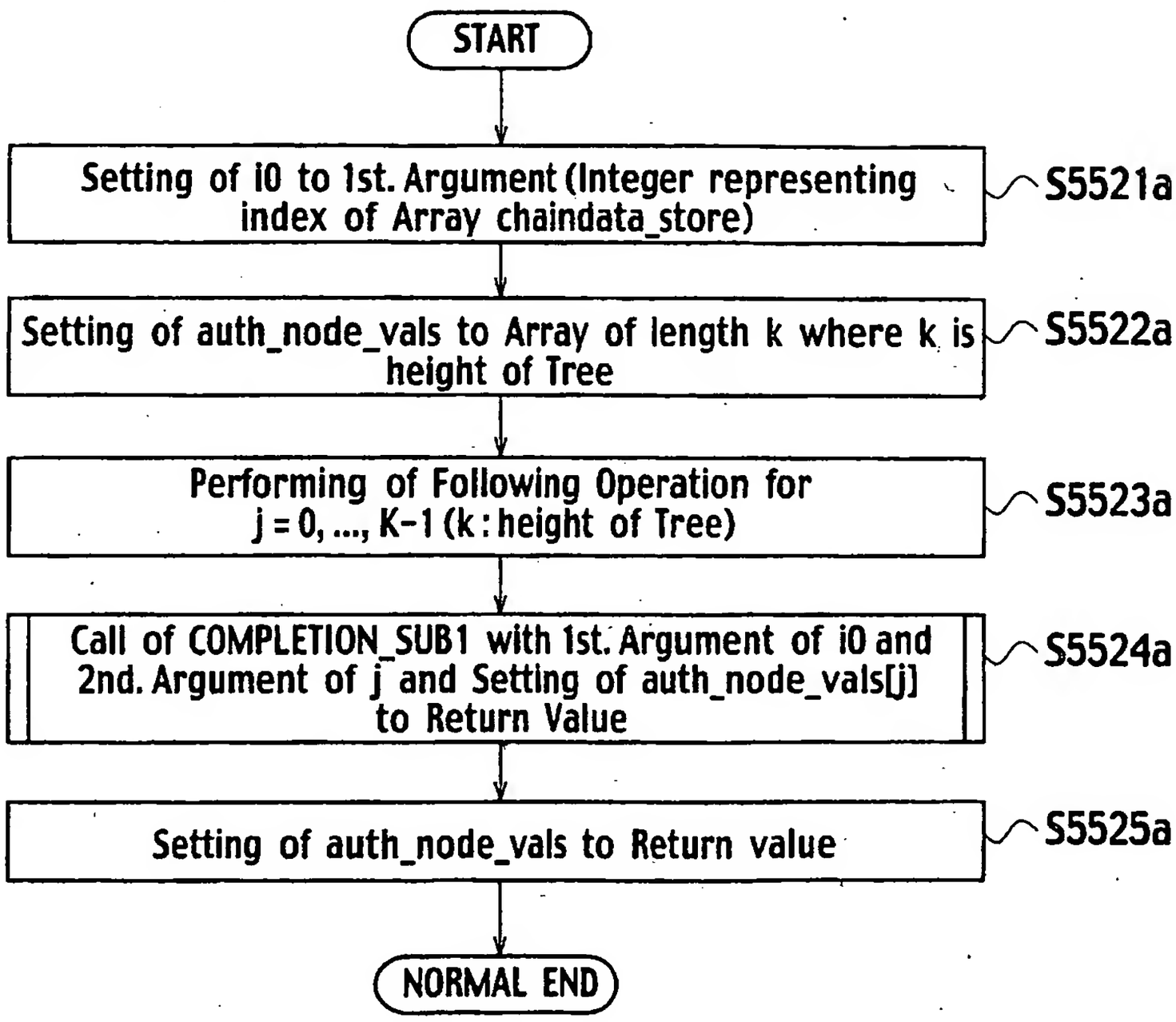

START
Setting of i0 to 1st. Argument (Integer representing index of Array chaindata_store)
S5521a
Setting of auth_node_vals to Array of length k where k is height of Tree
S5522a
Performing of Following Operation for j = 0, ..., K-1 (k : height of Tree)
S5523a
Call of COMPLETION_SUB1 with 1st. Argument of i0 and 2nd. Argument of j and Setting of auth_node_vals[j] to Return Value
S5524a
Setting of auth_node_vals to Return value
S5525a
NORMAL END

FIG. 68

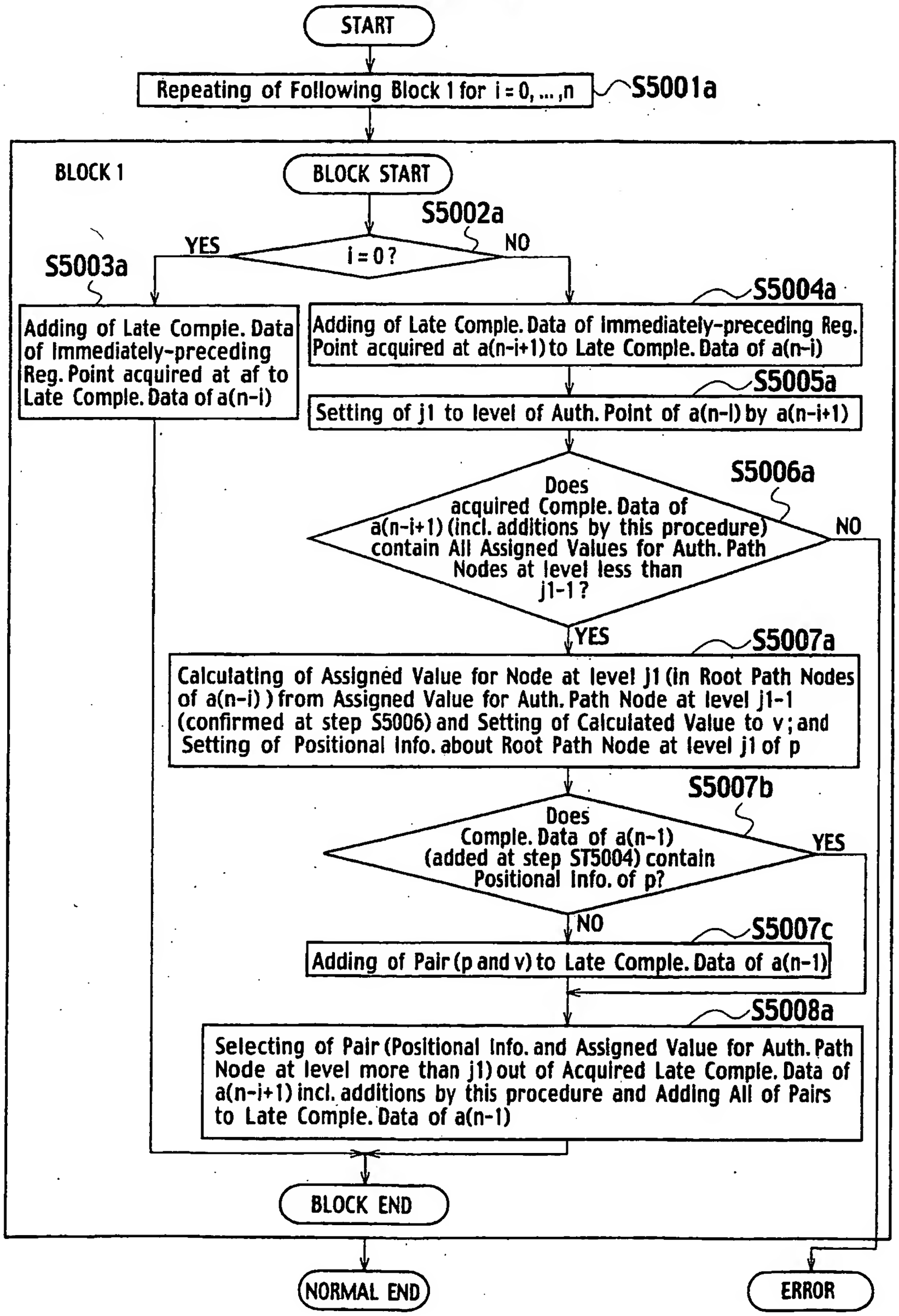

START
Repeating of Following Block 1 for i = 0, ... ,n
S5001a
BLOCK 1
BLOCK START
S5002a
i = 0 ?
YES
NO
S5003a
S5004a
Adding of Late Comple. Data of Immediately-preceding Reg. Point acquired at af to Late Comple. Data of a(n-i)
Adding of Late Comple. Data of Immediately-preceding Reg. Point acquired at a(n-i+1) to Late Comple. Data of a(n-i)
S5005a
Setting of j1 to level of Auth. Point of a(n-l) by a(n-i+1)
S5006a
Does acquired Comple. Data of a(n-i+1) (incl. additions by this procedure) contain All Assigned Values for Auth. Path Nodes at level less than j1-1 ?
NO
YES
S5007a
Calculating of Assigned Value for Node at level j1 (in Root Path Nodes of a(n-i)) from Assigned Value for Auth. Path Node at level j1-1 (confirmed at step S5006) and Setting of Calculated Value to v ; and Setting of Positional Info. about Root Path Node at level j1 of p
S5007b
Does Comple. Data of a(n-1) (added at step ST5004) contain Positional Info. of p?
YES
NO
S5007c
Adding of Pair (p and v) to Late Comple. Data of a(n-1)
S5008a
Selecting of Pair (Positional Info. and Assigned Value for Auth. Path Node at level more than j1) out of Acquired Late Comple. Data of a(n-i+1) incl. additions by this procedure and Adding All of Pairs to Late Comple. Data of a(n-1)
BLOCK END
NORMAL END
ERROR

FIG. 69

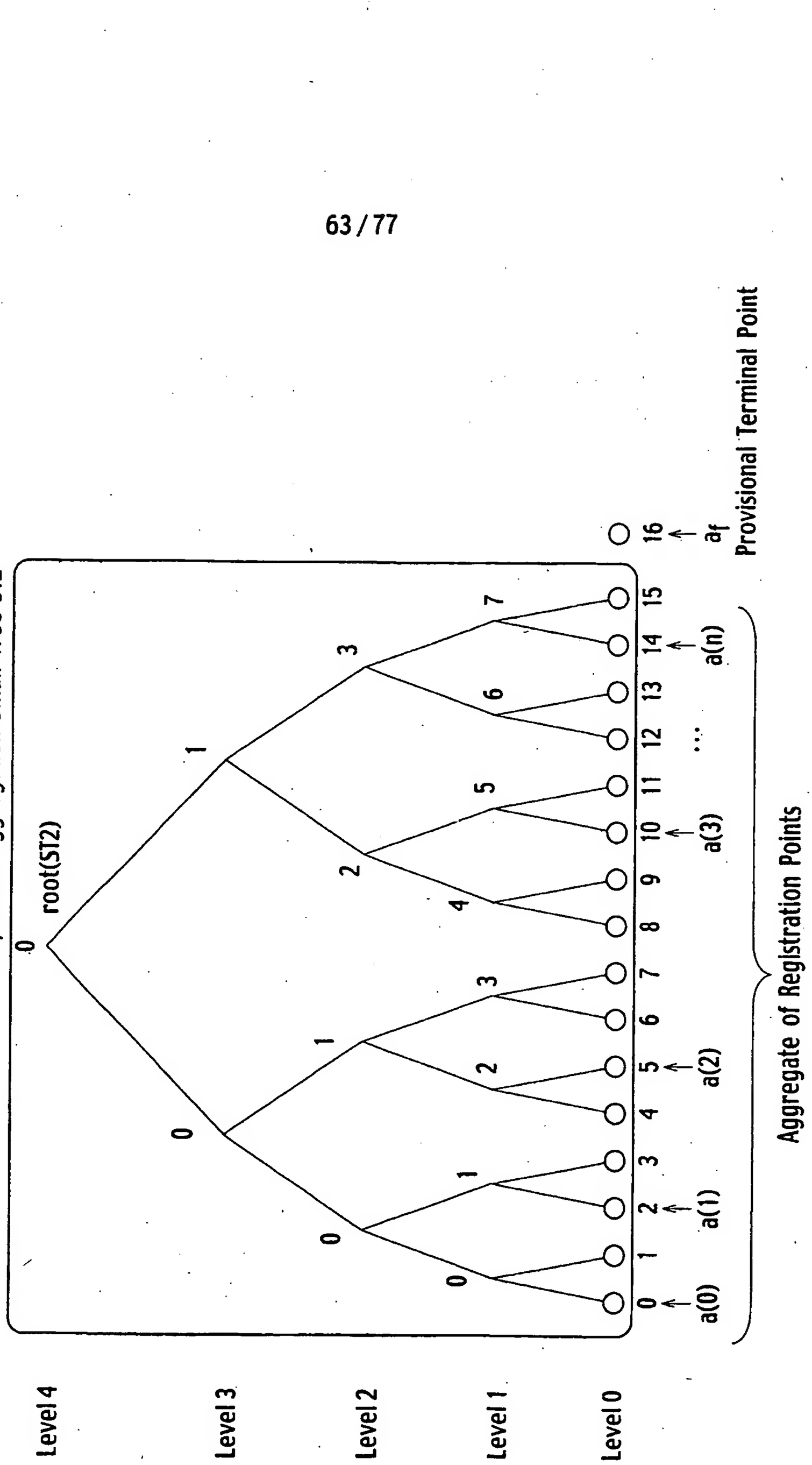

Sequential Aggregation Small Tree ST2
root(ST2)
Level 4
Level 3
Level 2
Level 1
Level 0
a(0)
a(1)
a(2)
a(3)
a(n)
af
Provisional Terminal Point
Aggregate of Registration Points

FIG. 70

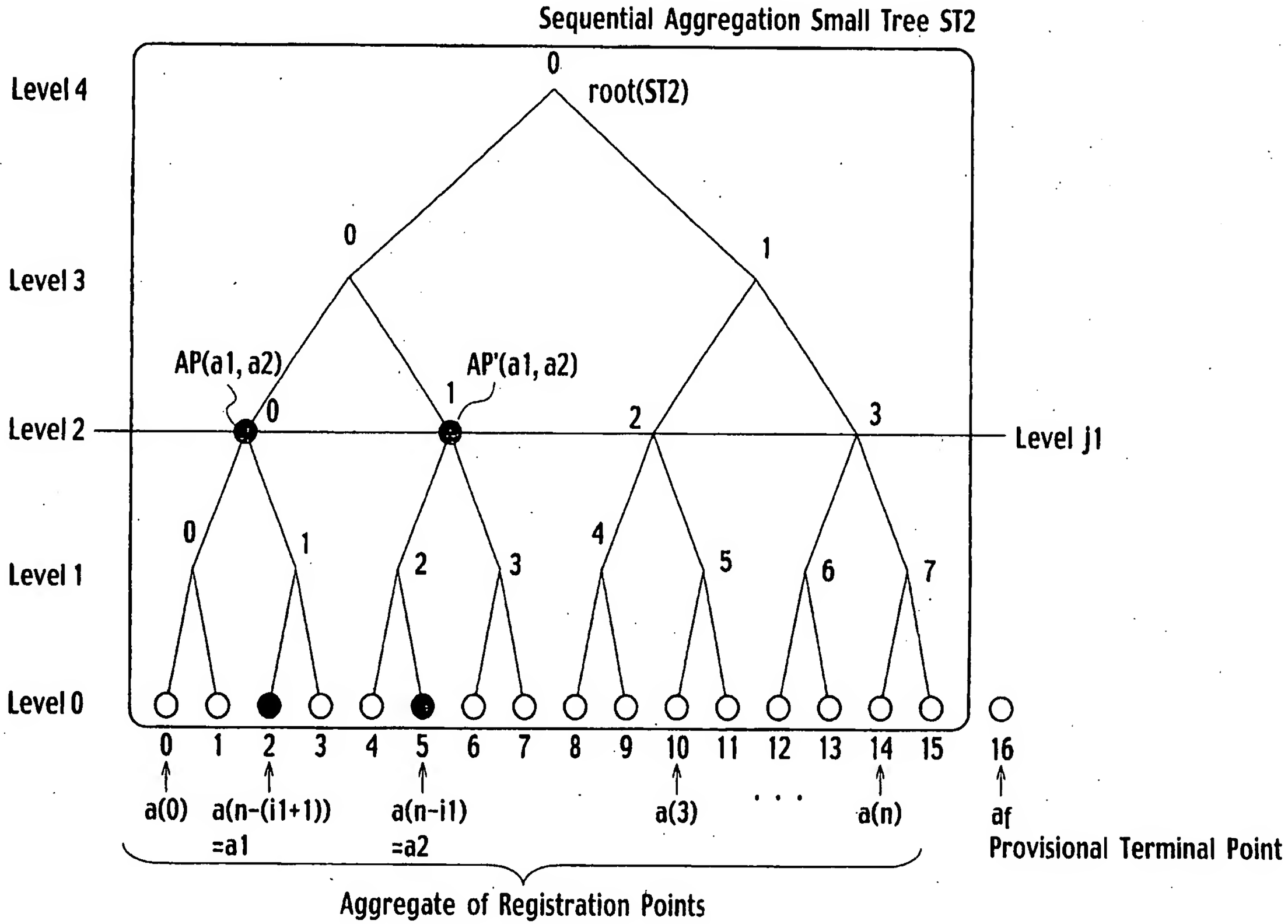

Sequential Aggregation Small Tree ST2
Level 4
Level 3
Level 2
Level 1
Level 0
root(ST2)
AP(a1, a2)
AP'(a1, a2)
Level j1
a(0)
a(n-(i1+1))
=a1
a(n-i1)
=a2
a(3)
a(n)
af
Provisional Terminal Point
Aggregate of Registration Points

FIG. 71

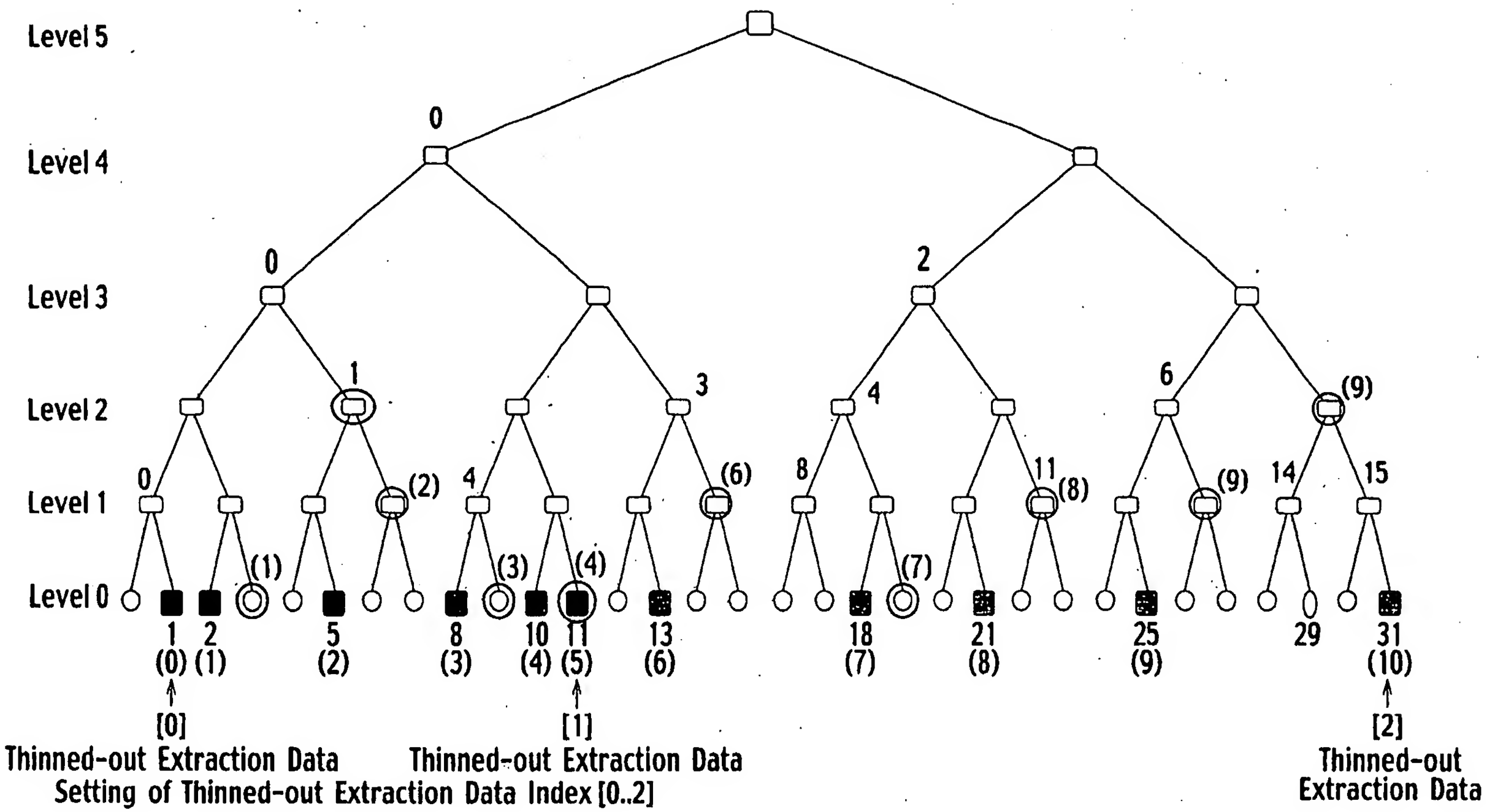

Level 5
Level 4
Level 3
Level 2
Level 1
Level 0
0
0
1
(2)
3
(6)
0
1
(1)
4
(3)
(4)
4
8
11
(8)
(7)
6
(9)
(9)
14
15
1 2
(0) (1)
5
(2)
8
(3)
10
(4)
11
(5)
13
(6)
18
(7)
21
(8)
25
(9)
29
31
(10)
[0]
[1]
[2]
Thinned-out Extraction Data
Setting of Thinned-out Extraction Data Index [0..2]
Thinned-out Extraction Data
Thinned-out Extraction Data

FIG. 72

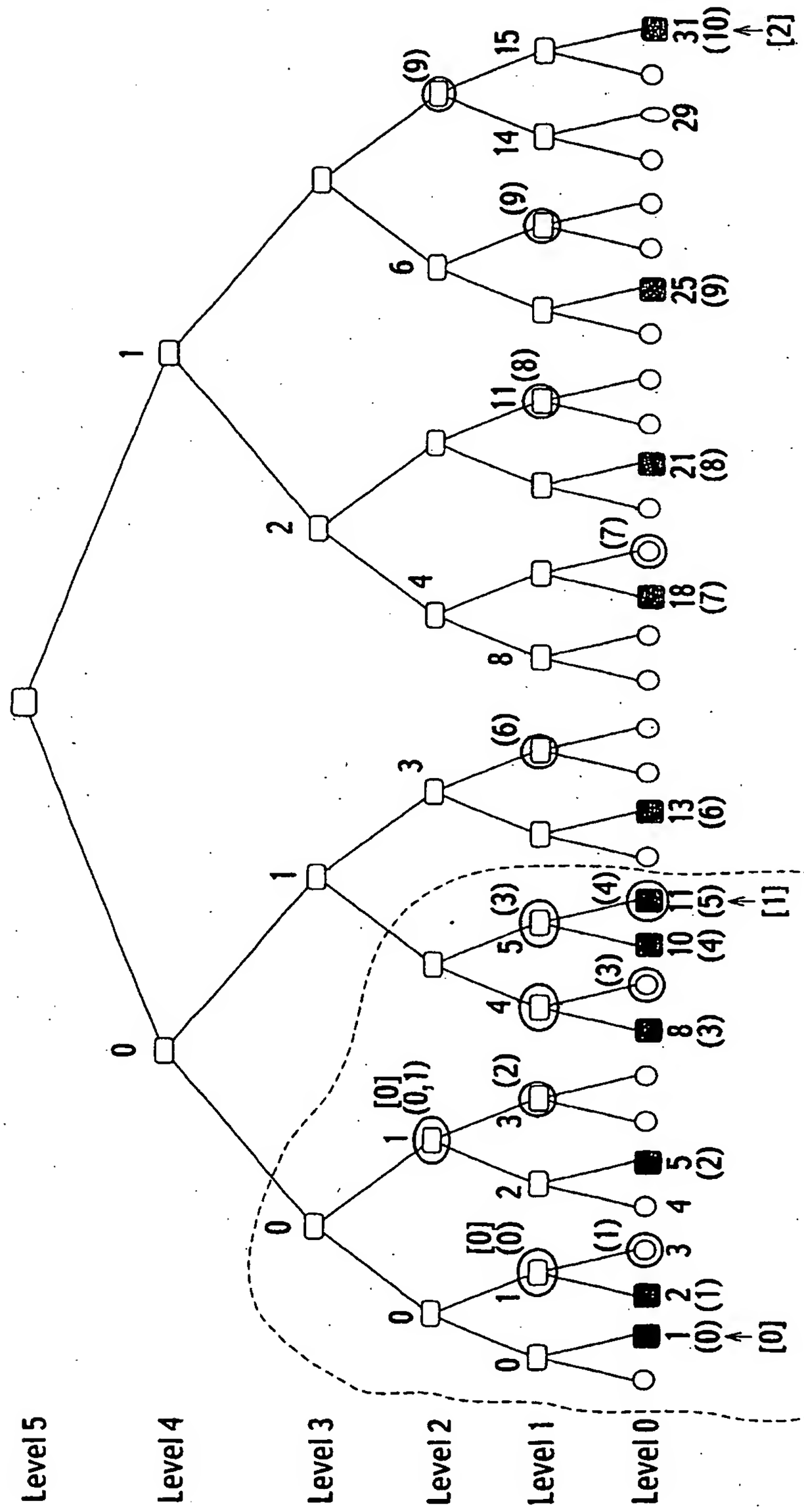
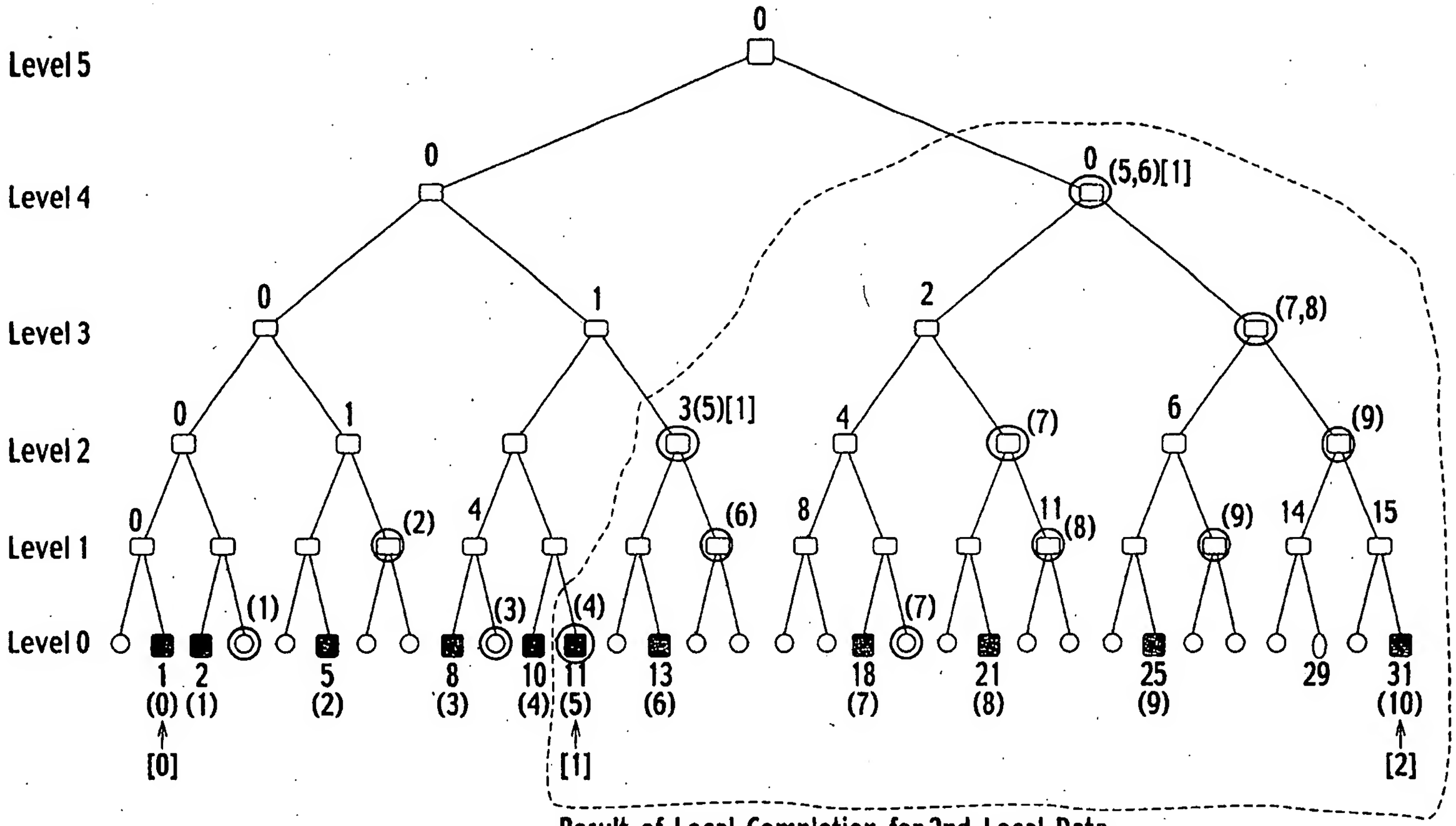

Level 5
Level 4
Level 3
Level 2
Level 1
Level 0
Result of Local Completion for 1st. Local Data
Range of Original Index for Local Completion [0..5]
Range of Thinned-out Extraction Data Index [0..1]

FIG. 73



Result of Local Completion for 2nd. Local Data
Range of Index for Local Completion [5..10]
Range of Thinned-out Extraction Data Index [1..2]

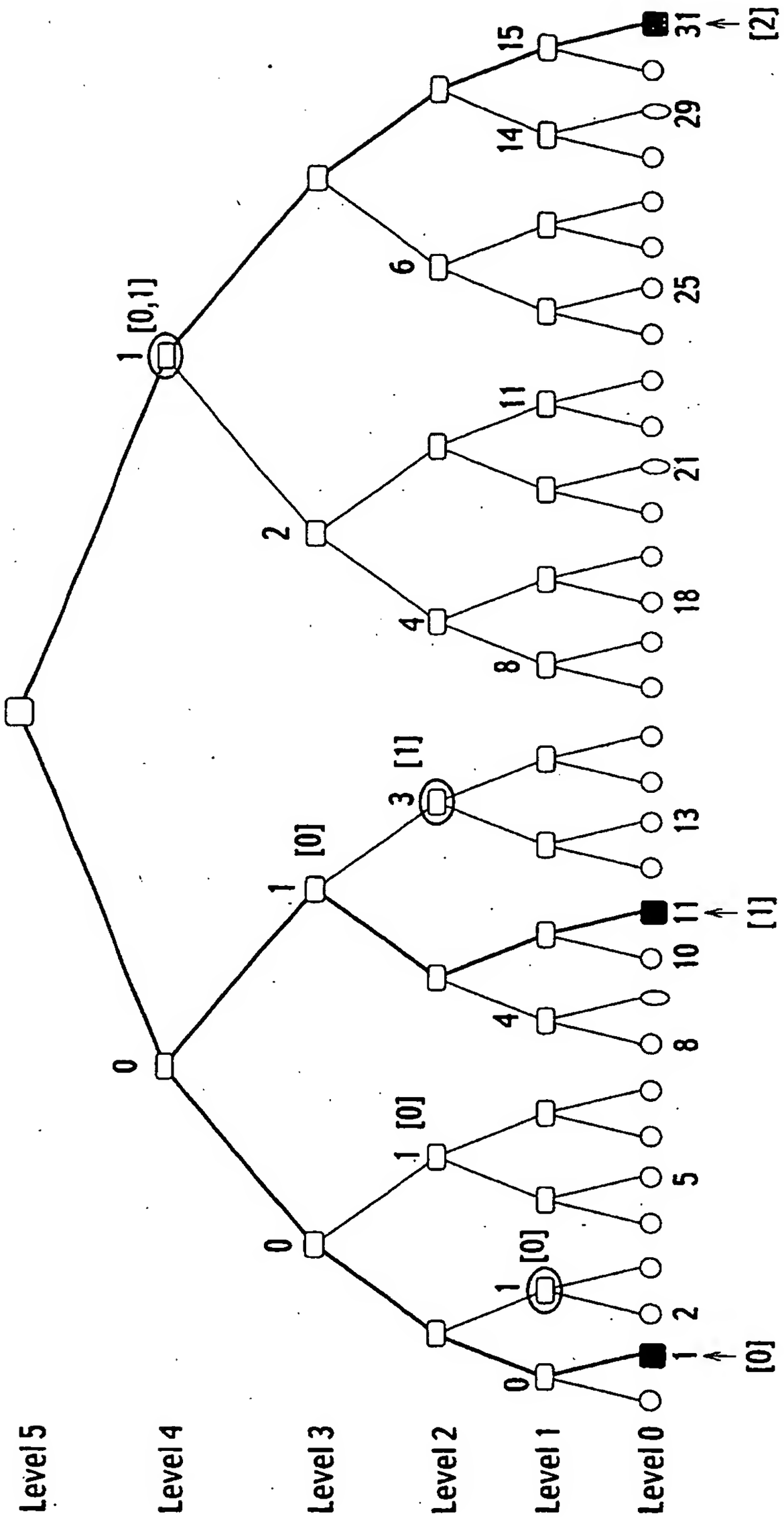

Level 5
Level 4
Level 3
Level 2
Level 1
Level 0
1 [0,1]
0
1
0
2
1 [0]
0
1 [1]
1
0
1 [0]
0
1
0
15
14
6
4
8
3 [1]
1
4
1 [0]
0
31 ← [2]
29
25
11
21
18
13
10 11 ← [1]
8
5
2
1 ← [0]

FIG. 74

FIG. 75

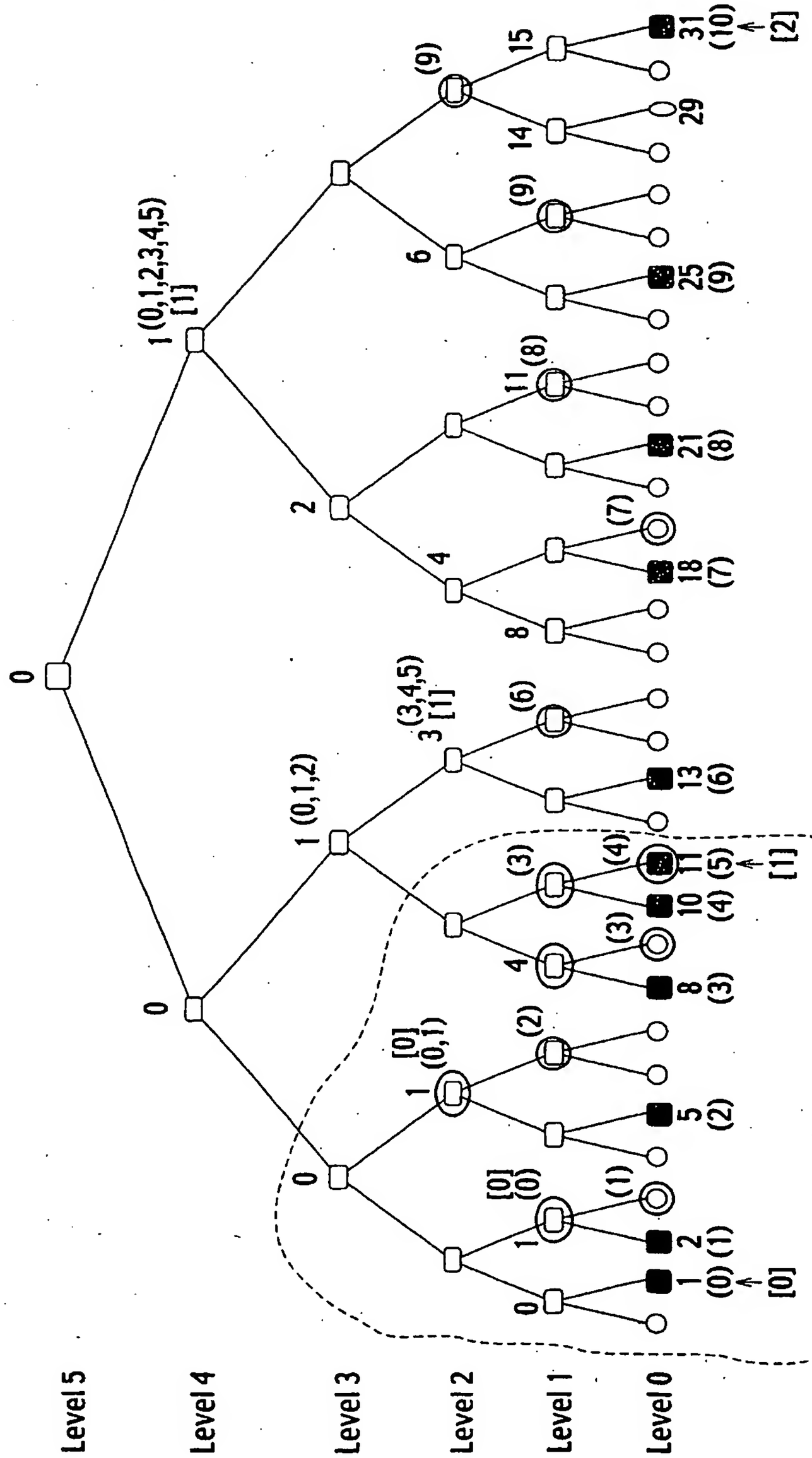

Level 5
Level 4
Level 3
Level 2
Level 1
Level 0
Result of Global Completion for 1st. Local data
Range of Index for Local Completion [0..5]

FIG. 76

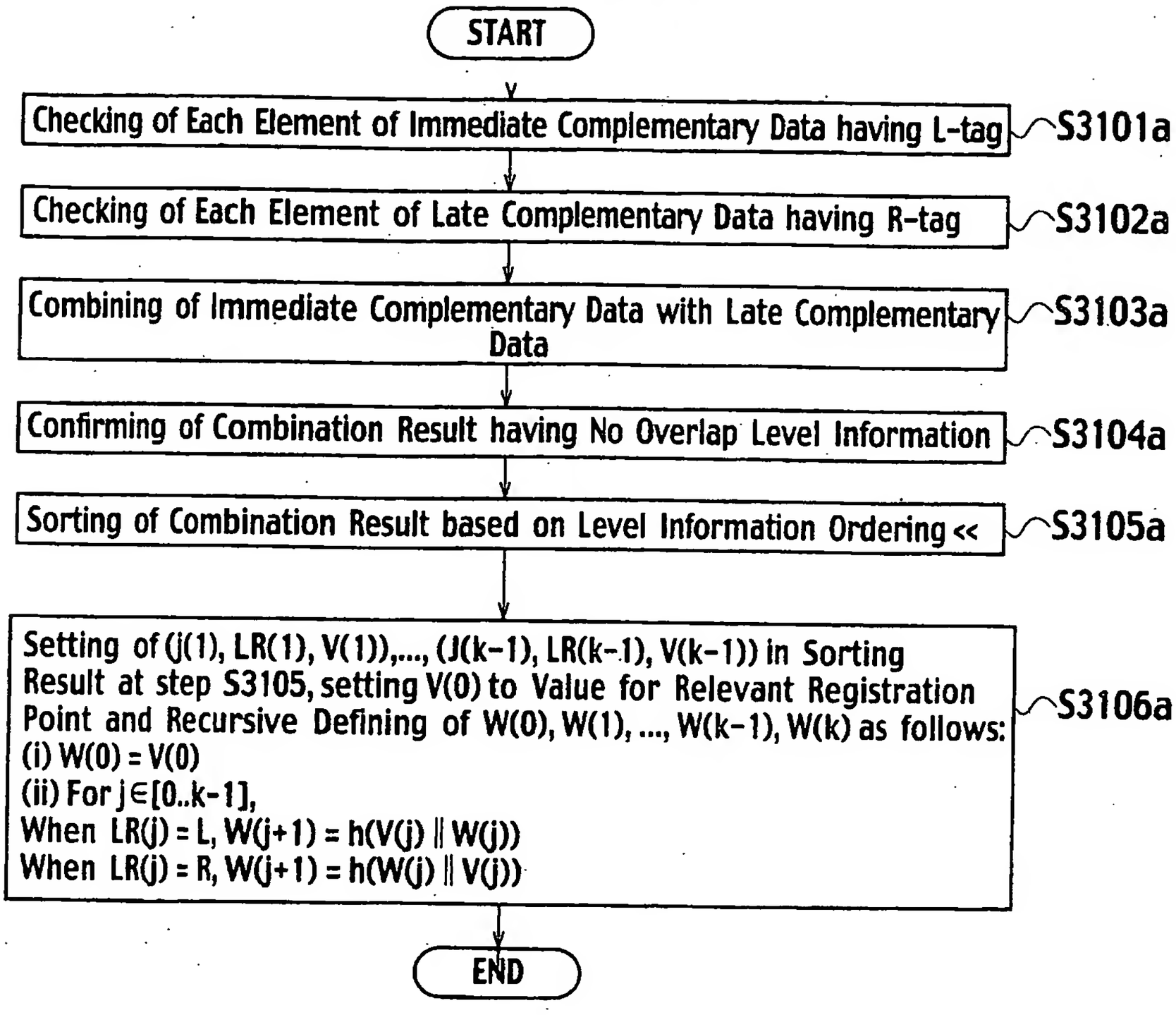
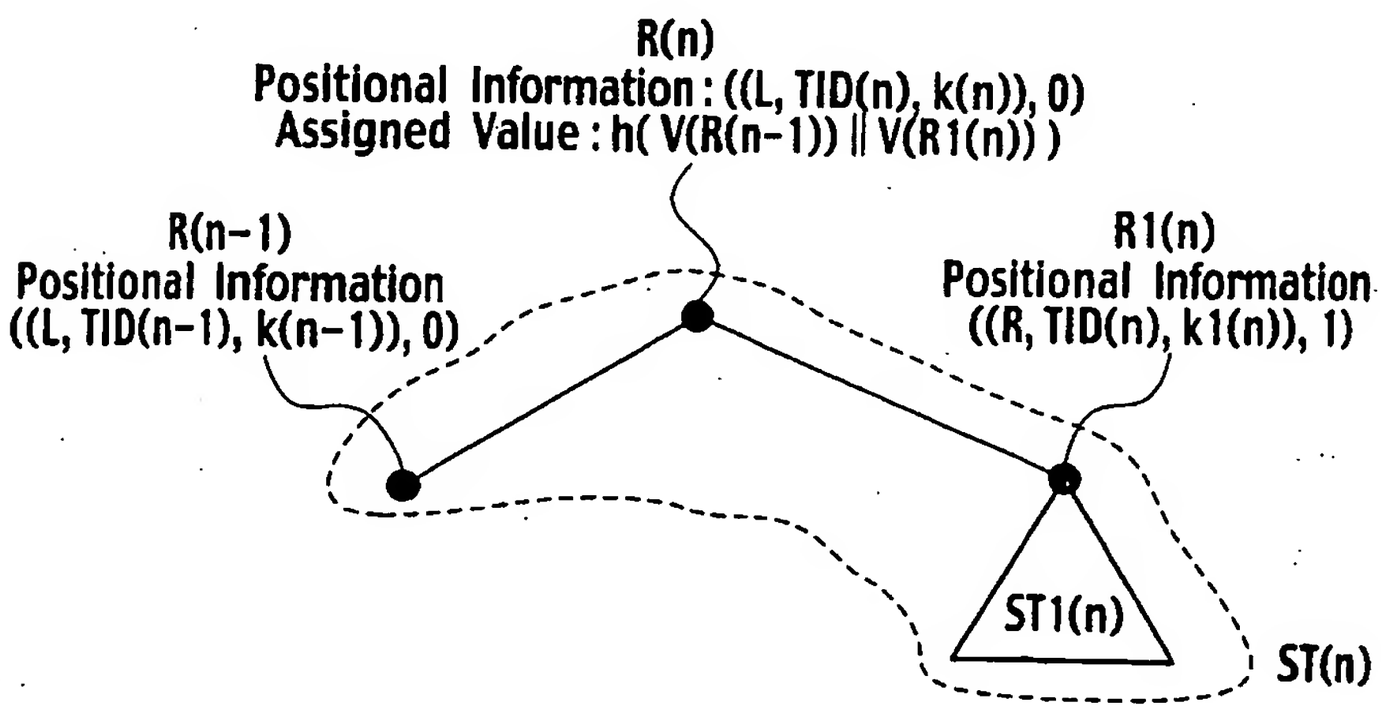

START
Checking of Each Element of Immediate Complementary Data having L-tag
S3101a
Checking of Each Element of Late Complementary Data having R-tag
S3102a
Combining of Immediate Complementary Data with Late Complementary Data
S3103a
Confirming of Combination Result having No Overlap Level Information
S3104a
Sorting of Combination Result based on Level Information Ordering <<
S3105a
Setting of (j(1), LR(1), V(1)),..., (J(k-1), LR(k-1), V(k-1)) in Sorting Result at step S3105, setting V(0) to Value for Relevant Registration Point and Recursive Defining of W(0), W(1), ..., W(k-1), W(k) as follows:
(i) W(0) = V(0)
(ii) For j∈[0..k-1],
When LR(j) = L, W(j+1) = h(V(j) || W(j))
When LR(j) = R, W(j+1) = h(W(j) || V(j))
S3106a
END

FIG. 77


R(n)
Positional Information : ((L, TID(n), k(n)), 0)
Assigned Value : h(V(R(n-1)) || V(R1(n)))
R(n-1)
Positional Information
((L, TID(n-1), k(n-1)), 0)
R1(n)
Positional Information
((R, TID(n), k1(n)), 1)
ST1(n)
ST(n)

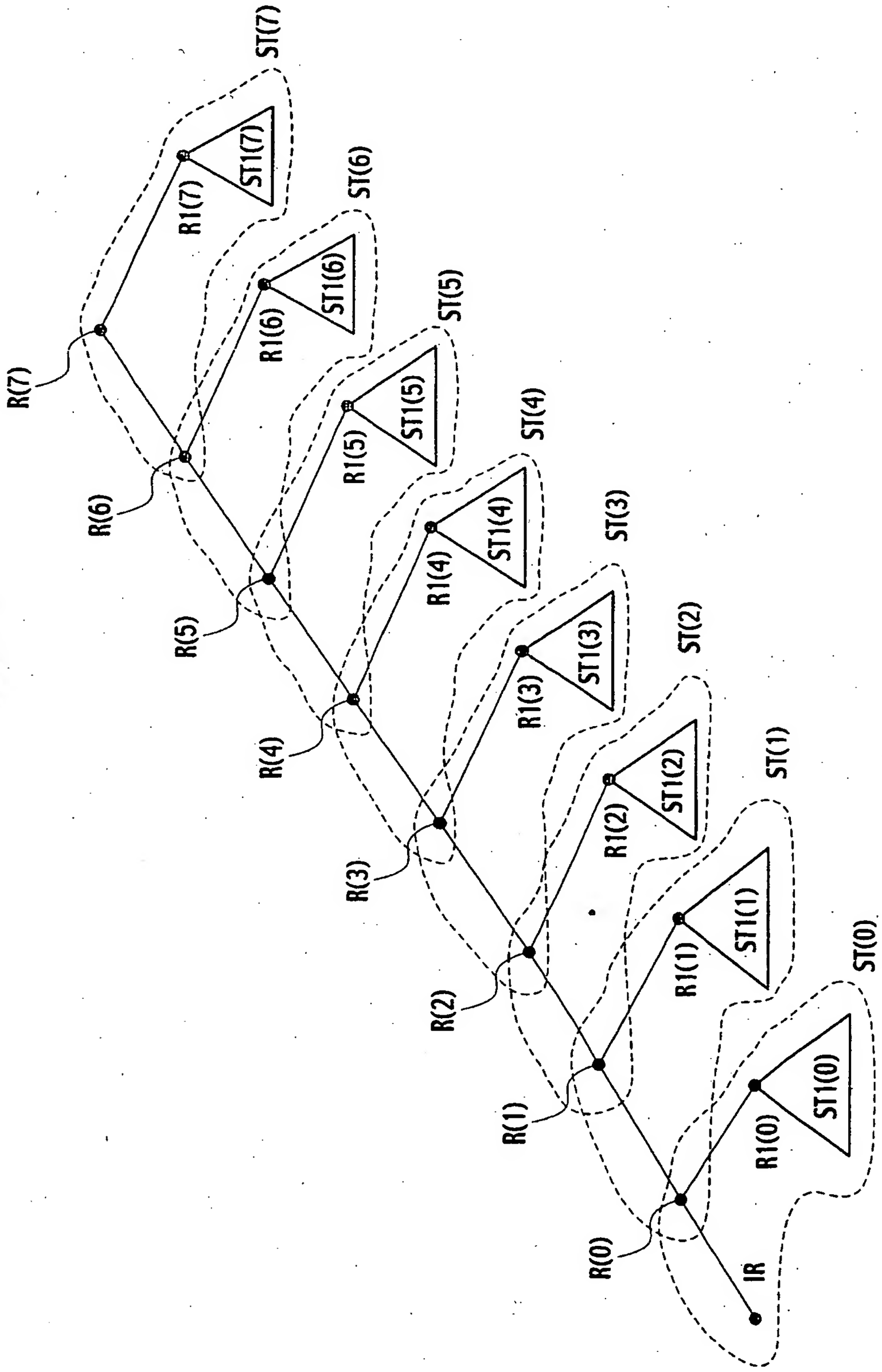

ST(7)
ST1(7)
R1(7)
R(7)
ST(6)
ST1(6)
R1(6)
R(6)
ST(5)
ST1(5)
R1(5)
R(5)
ST(4)
ST1(4)
R1(4)
R(4)
ST(3)
ST1(3)
R1(3)
R(3)
ST(2)
ST1(2)
R1(2)
R(2)
ST(1)
ST1(1)
R1(1)
R(1)
ST(0)
ST1(0)
R1(0)
R(0)
IR

FIG. 78

FIG. 79

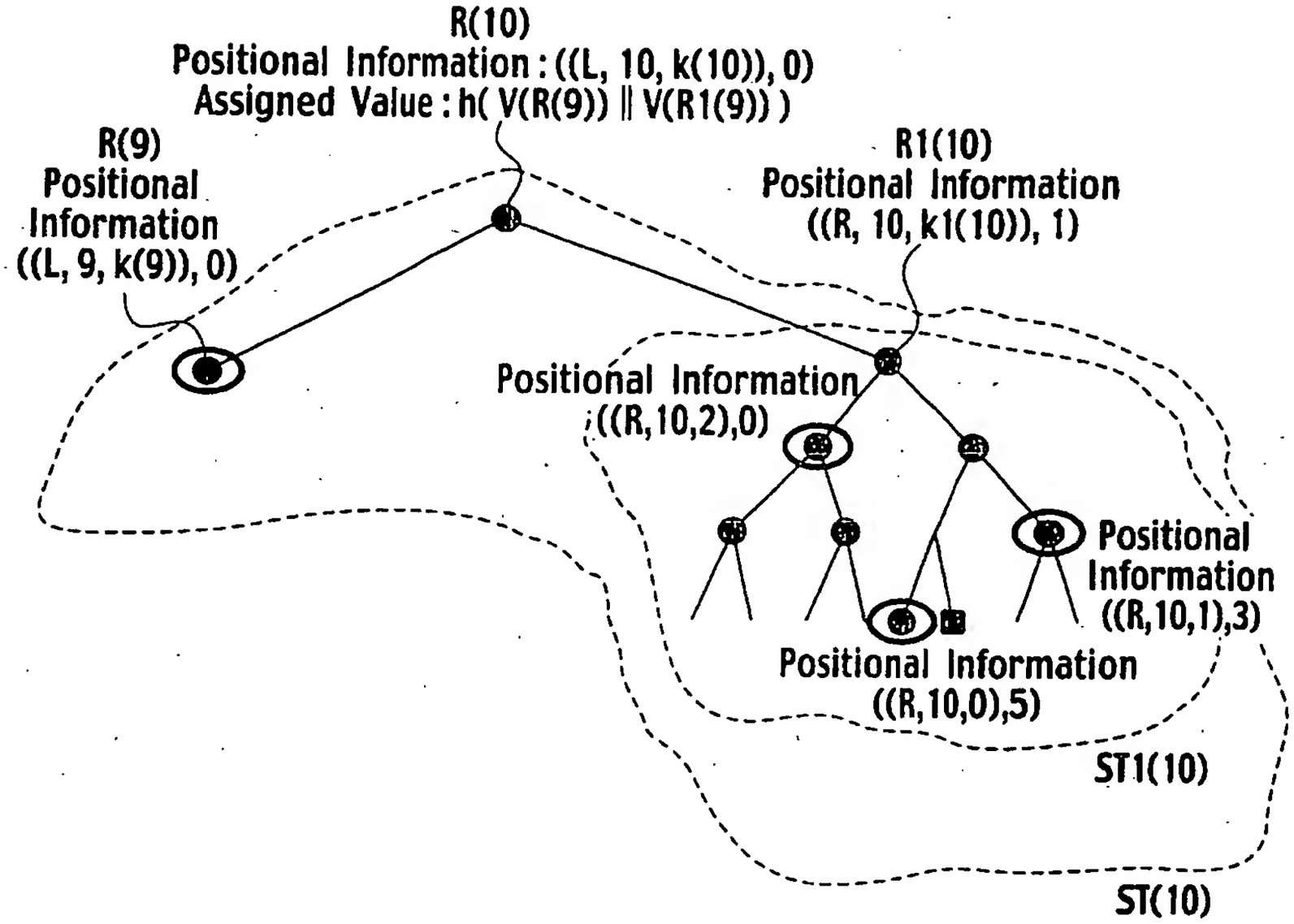

R(10)
Positional Information : ((L, 10, k(10)), 0)
Assigned Value : h(V(R(9)) || V(R1(9)))
R(9)
Positional
Information
((L, 9, k(9)), 0)
R1(10)
Positional Information
((R, 10, k1(10)), 1)
Positional Information
((R,10,2),0)
Positional
Information
((R,10,1),3)
Positional Information
((R,10,0),5)
ST1(10)
ST(10)

FIG. 80

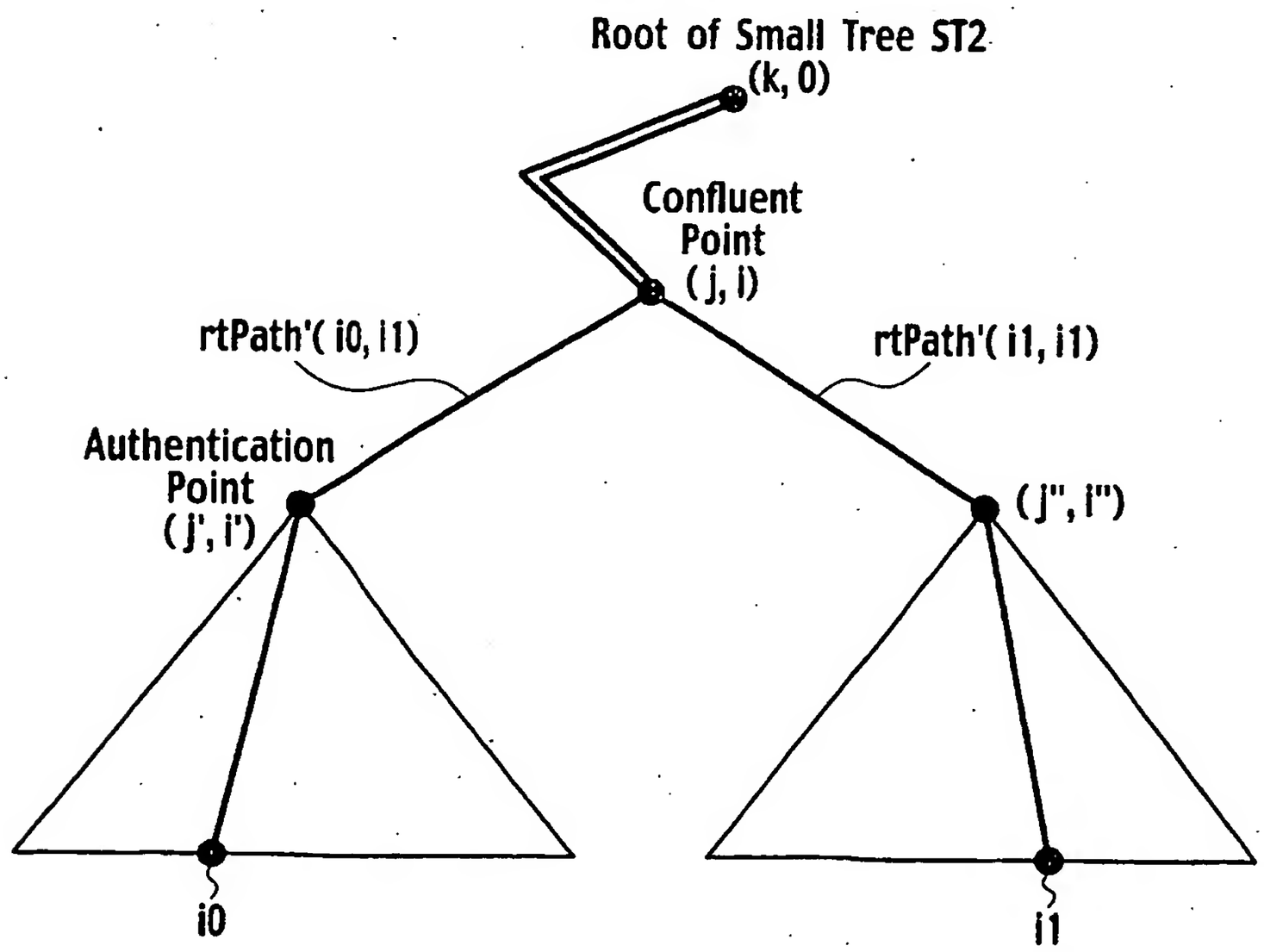

Root of Small Tree ST2
(k, 0)
Confluent
Point
(j, i)
rtPath'(i0, i1)
rtPath'(i1, i1)
Authentication
Point
(j', i')
(j'', i'')
i0
i1

FIG. 81

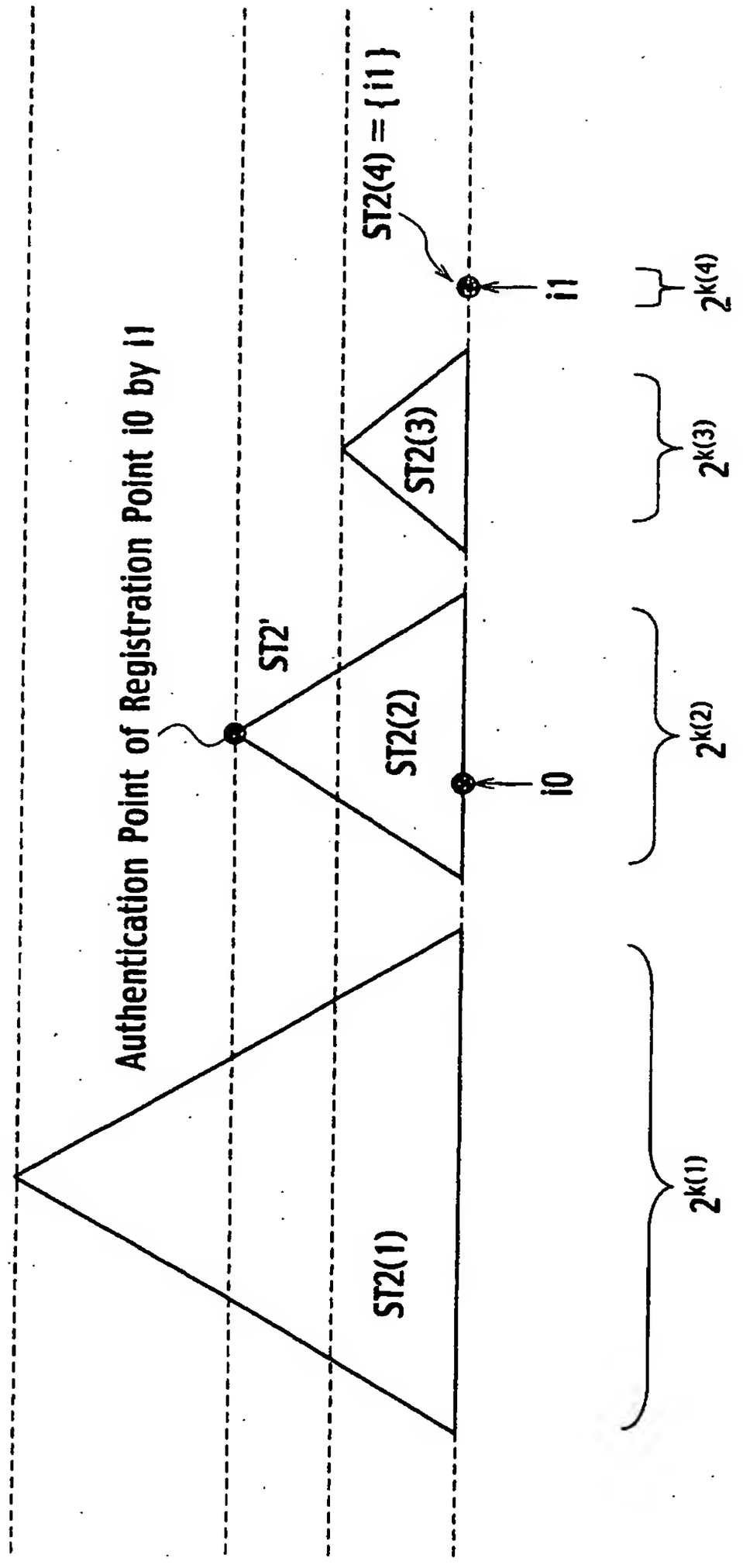

Authentication Point of Registration Point i0 by i1
ST2'
ST2(1)
ST2(2)
ST2(3)
ST2(4) = {i1}
i0
i1
2^k(1)
2^k(2)
2^k(3)
2^k(4)
k(1) > k(2) > k(3) > k(4) = 0

FIG. 82

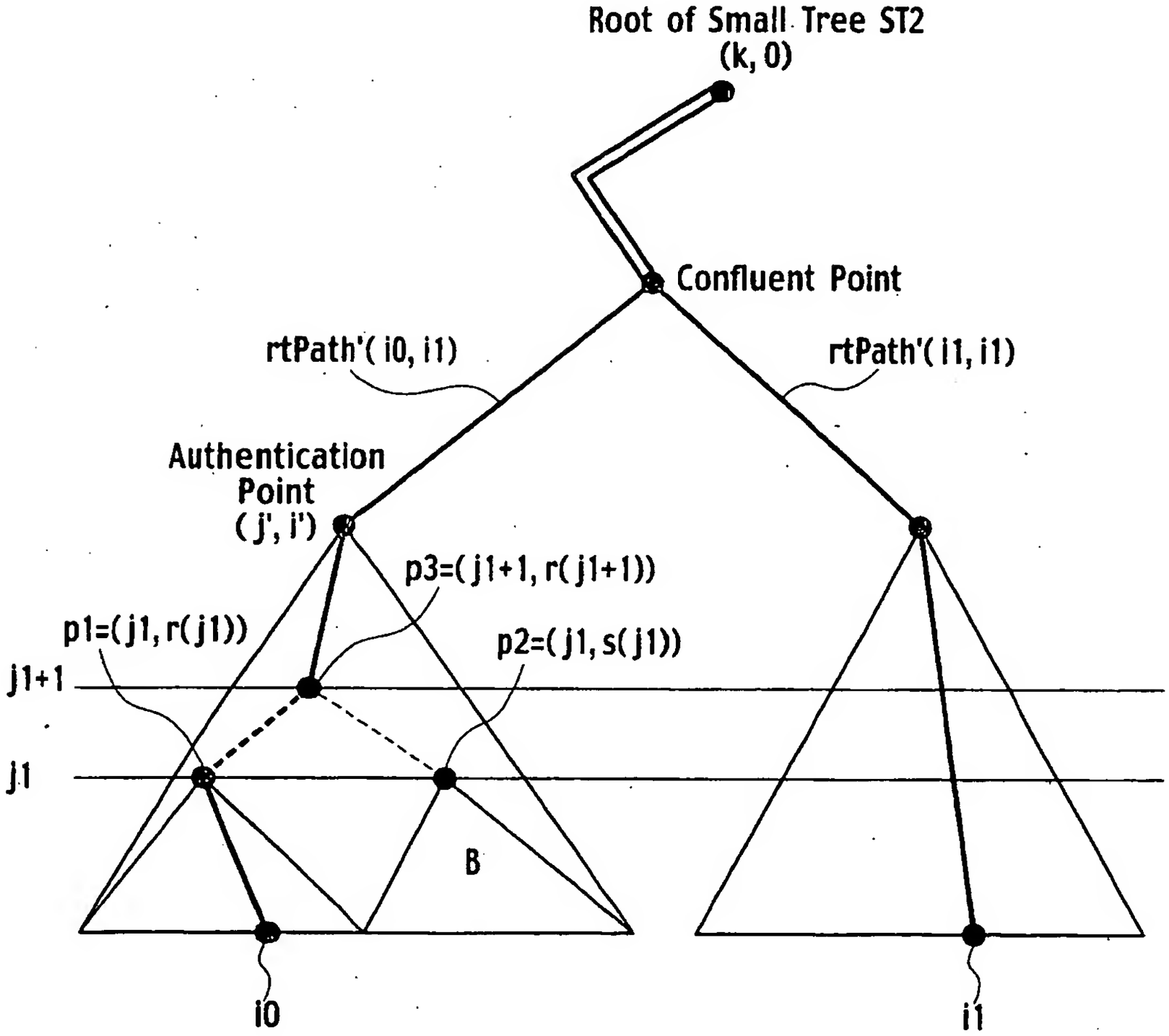

Root of Small Tree ST2
(k, 0)
Confluent Point
rtPath'(i0, i1)
rtPath'(i1, i1)
Authentication
Point
(j', i')
p3=(j1+1, r(j1+1))
p1=(j1, r(j1))
p2=(j1, s(j1))
j1+1
j1
B
i0
i1

FIG. 83

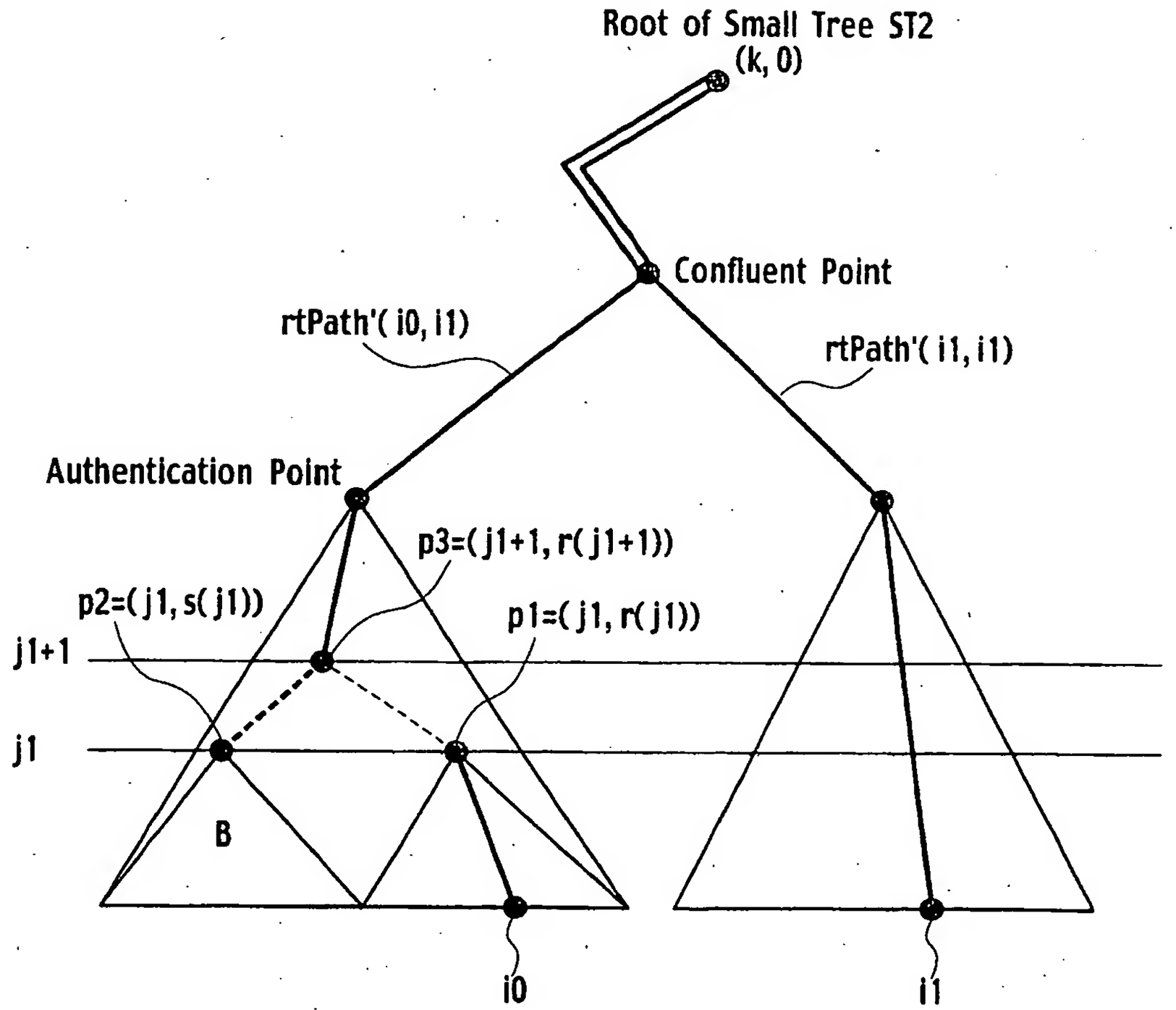

Root of Small Tree ST2
(k, 0)
Confluent Point
rtPath'(i0, i1)
rtPath'(i1, i1)
Authentication Point
p3=(j1+1, r(j1+1))
p2=(j1, s(j1))
p1=(j1, r(j1))
j1+1
j1
B
i0
i1

FIG. 84

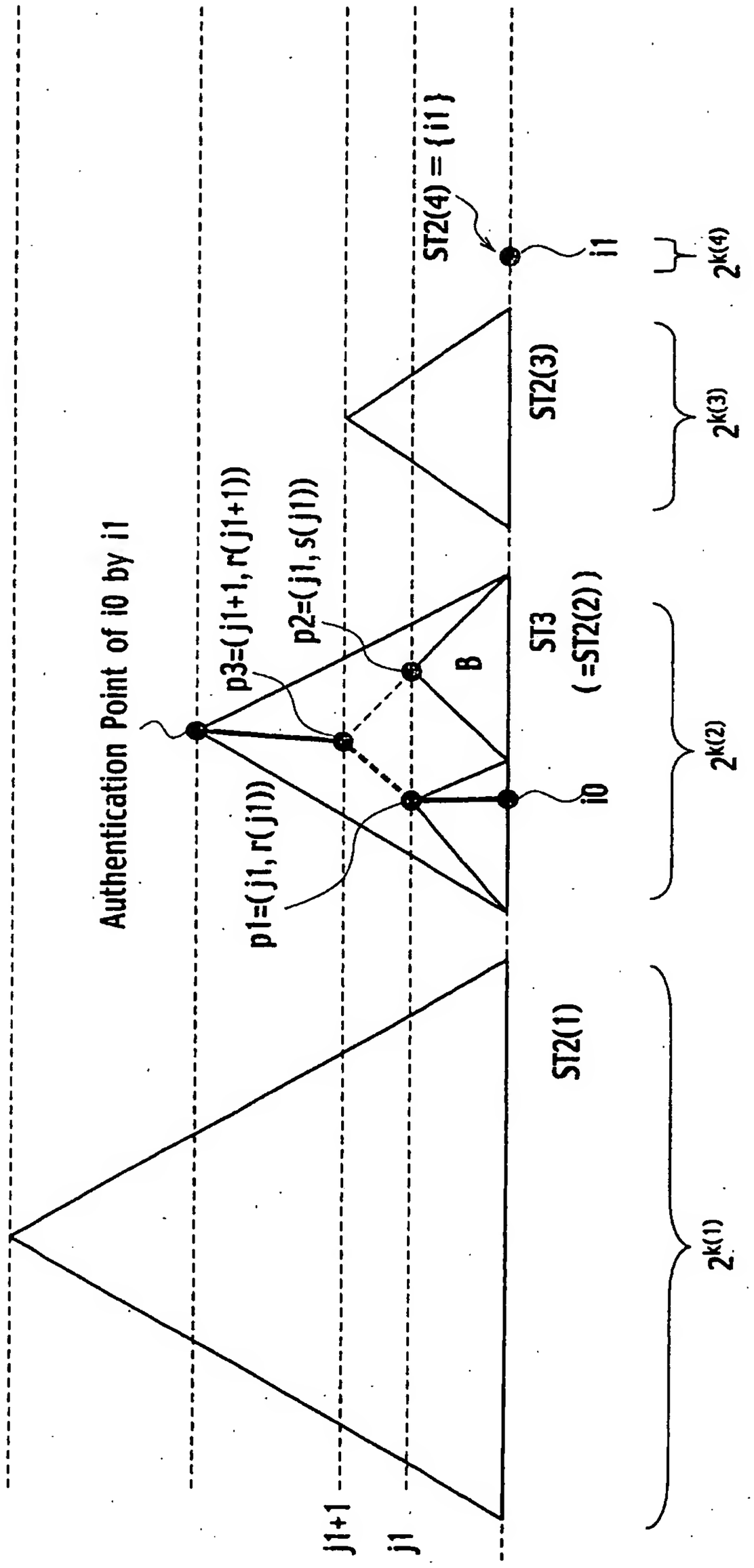
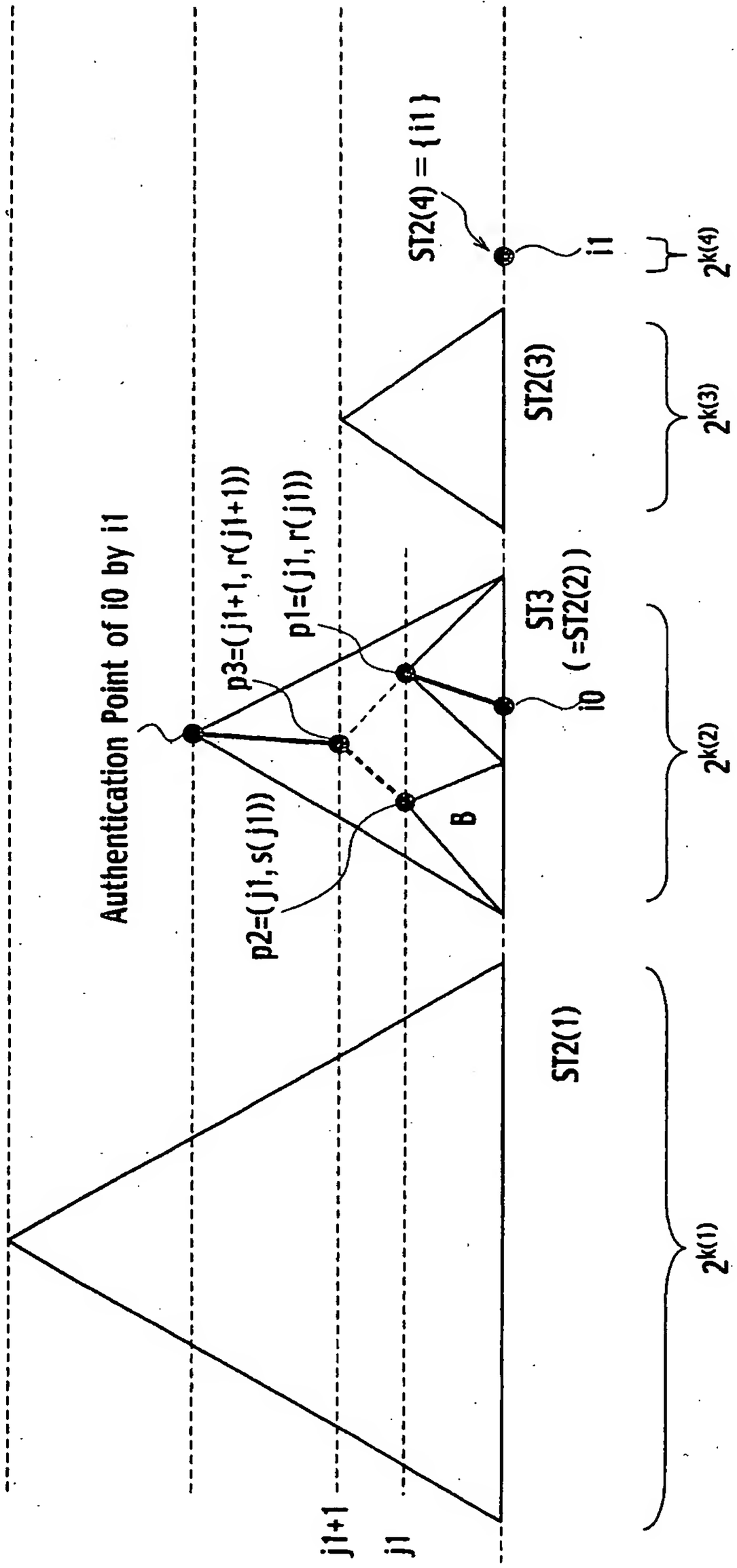

ST2(4) = {i1}
i1
2^k(4)
Authentication Point of i0 by i1
p3=(j1+1, r(j1+1))
p2=(j1, s(j1))
p1=(j1, r(j1))
B
ST3
(=ST2(2))
i0
ST2(3)
2^k(3)
2^k(2)
ST2(1)
2^k(1)
k(1) > k(2) > k(3) > k(4) = 0
j1+1
j1

FIG. 85


ST2(4) = {i1}
i1
2^k(4)
Authentication Point of i0 by i1
p3=(j1+1, r(j1+1))
p1=(j1, r(j1))
p2=(j1, s(j1))
B
ST3
i0 (=ST2(2))
ST2(3)
2^k(3)
2^k(2)
ST2(1)
2^k(1)
k(1)>k(2)>k(3)>k(4) = 0
j1+1
j1

CLAIMS

1. An event-ordering certification method for an event-ordering certification system having a user apparatus performing an event-ordering request for certifying a chronological sequence of a certain event in time-series events generating a designated digital information, a certification apparatus for drafting a certificate for the event-ordering request of the user apparatus, an audit apparatus for auditing authenticity of the certificate and a communication network for connecting the user apparatus, the certification apparatus and the audit apparatus with each other, the method comprising:

an event-ordering request receiving step where the certification apparatus receives the event-ordering request from the user apparatus;

a sequentially assigned data-item calculating step where the certification apparatus drafts a sequentially assigned data-item from the digital information included in the event-ordering request in accordance with a predetermined procedure;

an event-ordering request aggregating step where, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, the certification apparatus calculates assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

a certificate drafting step where the certification apparatus drafts a certificate containing the sequentially assigned data-item and a first sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned

thereto;

a certificate sending step where the certification apparatus sends the certificate to the user apparatus;

assuming that: a leaf of the sequential aggregation tree to which the event-ordering request is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the certificate; and in the complementary information, a complementary information acquirable at a point of assigning the event-ordering request to the sequential aggregation tree is defined as an immediate complementary information,

an audit certificate drafting step where after assigning the event-ordering request to the sequential aggregation tree, the certification apparatus assigns a first audit request to the sequential aggregation tree thereby drafting a first audit certificate in the same way as drafting the certificate, acquires a first immediate complementary information for audit at the point of assigning the first audit request to the sequential aggregation tree, from the sequential aggregation tree and incorporates the first immediate complementary information into the first audit certificate;

an audit certificate sending step where the certification apparatus sends the first audit certificate to the audit apparatus;

a complementary information request receiving step where after assigning the first audit request to the sequential aggregation tree, the certification apparatus receives a request of the complementary information of the certificate from the user apparatus;

a late complementary information drafting step where the certification apparatus acquires a second sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the request of the complementary information assigned thereto and a complementary information acquirable at the point of assigning the request of the complementary information, from the sequential aggregation tree, thereby forming a late

complementary information; and

a late complementary information sending step where the certification apparatus sends the late complementary information about the certificate to the user apparatus.

2. The event-ordering certification method of claim 1, wherein at the certificate drafting step, the certification apparatus incorporates the immediate complementary information of the certificate into the first sequential aggregation tree specifying information.

3. The event-ordering certification method of claim 1 or 2, wherein:

the audit certificate drafting step further includes a step where before assigning the event-ordering request to the sequential aggregation tree, the certification apparatus assigns a second audit request to the sequential aggregation tree thereby drafting a second audit certificate in the same way as drafting the certificate, acquires a second immediate complementary information for audit at the point of assigning the second audit request to the sequential aggregation tree, from the sequential aggregation tree and incorporates the second immediate complementary information into the second audit certificate; the event-ordering certification method further comprising:

an audit late complementary information drafting step where after completing the regular time interval, the certification apparatus acquires all of the complementary information about the first and second audit certificates drafted at the audit certificate drafting step, from the sequential aggregation tree thereby forming a late complementary information about the first and second audit certificates; and

an audit late complementary information sending step where the certification apparatus sends the late complementary information about the first and second audit certificates to the audit apparatus.

4. The event-ordering certification method of any one of claims 1 to 3, wherein at the sequentially assigned data-item calculating step, the sequentially assigned data-item calculated by the certification apparatus comprises a result value obtained by applying a designated collision-resistant hash function on the digital information contained in the event-ordering request.

5. The event-ordering certification method of any one of claims 1 to 4, wherein at the certificate drafting step, the certification apparatus applies a digital signature on the certificate drafted.

6. The event-ordering certification method of any one of claims 1 to 5, further comprising an electronic information publishing step where the certification apparatus electronically publishes the root value of the sequential aggregation tree after completing the regular time interval.

7. The event-ordering certification method of any one of claims 1 to 6, wherein for a plurality of event-ordering requests from the user apparatus, the certificate sending step further includes a step where the certification apparatus sends respective certificates for the event-ordering requests in chronological sequence of assigning the event-ordering requests to the sequential aggregation tree.

8. The event-ordering certification method of claim 2, further comprising, for a plurality of event-ordering requests from the user apparatus:

a sequential aggregation tree storing step where the certification apparatus stores an information about the sequential aggregation tree produced at the event-ordering request aggregating step; and,

assuming that: the late complementary information of a leaf a1 determined at the point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary

information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

a registration point storing step where the certification apparatus stores an information about the registration points of the plural event-ordering requests, wherein

at the certificate drafting step, the certification apparatus drafts a certificate for the new registration point from the information stored at both of the sequential aggregation tree storing step and the registration point storing step by integrating: the sequential assigned data-item of the new registration point; the first sequential aggregation tree specifying information for specifying the sequential aggregation tree and the leaf thereof both having the sequentially assigned data-item assigned thereto; the immediate complementary information of the new registration point; and the late complementary information of all of the passed registration points of the user apparatus at the new registration point.

9. The event-ordering certification method of claim 2, further comprising, for a plurality of event-ordering requests from the user apparatus:

a sequential aggregation tree storing step where the certification apparatus stores an information about the sequential aggregation tree produced at the event-ordering request aggregating step; and,

assuming that: the late complementary information of a leaf a1 determined at the point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

a registration point storing step where the certification apparatus stores an information about an immediately preceding registration point to the new registration point, wherein

at the certificate drafting step, the certification apparatus drafts a certificate for the new registration point from the information stored at both of the sequential aggregation tree storing step and the registration point storing step by integrating: the sequential assigned data-item of the new registration point; the sequential aggregation tree specifying information for specifying the sequential aggregation tree and the leaf thereof both having the sequentially assigned data-item assigned thereto; the immediate complementary information of the new registration point; and the late complementary information of the immediately preceding registration point of the user apparatus at the new registration point.

10. The event-ordering certification method of claim 8 or 9, wherein at the sequential aggregation tree storing step, the certification apparatus stores respective positions of nodes in the sequential aggregation tree, which have been subjected to an assignation, and respective assigned values for the nodes, as the information about the sequential aggregation tree.

11. The event-ordering certification method of claim 9, wherein the certification apparatus stores the immediate complementary information of the new registration point and the late complementary information of the immediately preceding registration point of the user apparatus at the new registration point, individually in stack.

12. The event-ordering certification method of any one of claims 8 to 11, further comprising an electronic information publishing step where the certification apparatus electronically publishes the root value of the sequential aggregation tree after completing the regular time interval.

13. The event-ordering certification method of any one of claims 8 to 12, further comprising a user's side electronic information publishing step where when the certification apparatus stops an operation thereof or vanishes data

necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval, the user apparatus electronically publishes both positional information and assigned values for one or more nodes whose assigned values are calculable and whose parents' assigned values are not calculable, from the certificates that the user apparatus has already received and stored by the time of stopping the operation of the certification apparatus or vanishing the data.

14. The event-ordering certification method of any one of claims 8 to 13, wherein at the event-ordering request aggregating step after completing the regular time interval, the certification apparatus assigns the root value of the sequential aggregation tree to a leaf of a next sequential aggregation tree so as to form the immediate complementary information about a new registration point assigned to the leaf of the next sequential aggregation tree.

15. An event-ordering certification audit method for an event-ordering certification system having at least one user apparatus performing an event-ordering request for certifying a chronological sequence of a certain event in time-series events generating a designated digital information, a certification apparatus for drafting a certificate for the event-ordering request of the user apparatus, an audit apparatus for auditing authenticity of the certificate and a communication network for connecting the user apparatus, the certification apparatus and the audit apparatus with each other, the method comprising:

an event-ordering request receiving step where the certification apparatus receives a first event-ordering request from the user apparatus;

a sequentially assigned data-item calculating step where the certification apparatus drafts a sequentially assigned data-item from a digital information included in the first event-ordering request in accordance with a predetermined procedure;

an event-ordering request aggregating step where, in sequential

aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, the certification apparatus calculates assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

a certificate drafting step where the certification apparatus drafts a first certificate containing the sequentially assigned data-item and a first sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto;

a certificate sending step where the certification apparatus sends the first certificate to the user apparatus;

assuming that: a leaf of the sequential aggregation tree to which the first event-ordering request is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the first certificate; and in the complementary information, a complementary information acquirable at a point of assigning the first event-ordering request to the sequential aggregation tree is defined as an immediate complementary information,

an audit certificate drafting step where the certification apparatus assigns a plurality of audit requests to the sequential aggregation tree thereby drafting a plurality of audit certificates in the same way as drafting the certificate, acquires immediate complementary information for audit at the point of assigning the respective audit requests to the sequential aggregation tree, from the sequential aggregation tree and incorporates the immediate complementary information for audit into the respective audit certificates;

an audit certificate sending step where the certification apparatus sends the audit certificates to the audit apparatus;

a complementary information request receiving step where after sending the first certificate to the user apparatus, the certification apparatus receives a request of the complementary information of the first certificate from the user apparatus;

a late complementary information drafting step where the certification apparatus acquires a second sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the request of the complementary information assigned thereto and a complementary information acquirable at the point of assigning the request of the complementary information, from the sequential aggregation tree, thereby forming a late complementary information;

a late complementary information sending step where the certification apparatus sends the late complementary information about the first certificate to the user apparatus;

an audit certificate receiving step where the audit apparatus receives the audit certificates from the certification apparatus;

an audit request receiving step where the audit apparatus receives an audit request for the first certificate from the user apparatus, the audit request containing the first certificate and the late complementary information about the first certificate;

a first audit certificate selecting step where the audit apparatus selects an audit certificate from the audit certificates on a basis of the first and second sequential aggregation tree specifying information in the audit request for the first certificate, the one audit certificate being generated after the first certificate and before the late complementary information in chronological sequence;

a first certificate audit step where the audit apparatus audits validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit certificate

selected at the first audit certificate selecting step coincides with an assigned value for the specified node calculated from the audit request for the first certificate or not and, where the audit apparatus further certifies a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt time of the audit request for the audit certificate selected at the first audit certificate selecting step; and

an audit result sending step where the audit apparatus sends an audit result of the first certificate to the user apparatus.

16. The event-ordering certification audit method of claim 15, wherein:

the audit certificate receiving step further includes a step of acquiring a first time when the audit apparatus received the audit certificate selected at the first audit certificate selecting step, from a time offering apparatus; and

at the first certificate audit step, the audit apparatus incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first certificate is temporally ahead of the first time into the audit result.

17. The event-ordering certification audit method of claim 15 or 16, further comprising

an audit late complementary information drafting step where after completing the regular time interval, the certification apparatus acquires all of the complementary information about the audit certificates drafted at the audit certificate drafting step, from the sequential aggregation tree thereby forming a late complementary information about the audit certificates;

an audit late complementary information sending step where the certification apparatus sends the late complementary information about the audit certificates to the audit apparatus;

a second audit certificate selecting step where the audit apparatus selects an audit certificate from the audit certificates on a basis of the first sequential

aggregation tree specifying information in the audit request for the first certificate, the audit certificate being generated before the first certificate in chronological sequence; and

a second certificate audit step where the audit apparatus audits validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit request for the first certificate coincides with an assigned value for the specified node calculated from the audit certificate selected at the second audit certificate selecting step and the late complementary information in the audit certificate or not and, where the audit apparatus further certifies a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt time of the audit request for the audit certificate selected at the second audit certificate selecting step.

18. The event-ordering certification audit method of claim 17, further comprising, for a second event-ordering request from the user apparatus or the other user apparatus, an inter-certificate ordering judgment step where the audit apparatus judges the temporal context between the receipt time of the event-ordering request for the first certificate and the receipt time of the event-ordering request for the second certificate on a basis of validation of the audit result for the second certificate drafted for the second event-ordering request and the first sequential aggregation tree specifying information about the first and second certificates, wherein

at the audit result sending step, the audit apparatus incorporates a chronological sequence in receiving the requests in between the plural certificates into the audit result.

19. The event-ordering certification audit method of claim 17 or 18, further comprising:

a root-value calculating step where the audit apparatus calculates a root

value of the sequential aggregation tree from the plural audit certificates and the late complementary information about the plural audit certificates; and

a root-value validation step where the audit apparatus verifies whether a root value of the sequential aggregation tree published electronically coincides with the root value calculated at the root-value calculating step.

20. The event-ordering certification audit method of any one of claims 17 to 19, further comprising an audit complementary information sending step where the audit apparatus sends the audit certificate selected at the first audit certificate selecting step and the late complementary information about the audit certificate to the user apparatus.

21. The event-ordering certification audit method of any one of claims 17 to 20, wherein:

the audit certificate receiving step further includes a step of acquiring a second time when the audit apparatus sent the audit certificate selected at the second audit certificate selecting step to the user apparatus, from a time offering apparatus; and

at the second certificate audit step, the audit apparatus incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first certificate is temporally ahead of the second time into the audit result.

22. The event-ordering certification audit method of any one of claims 15 to 21, wherein at the first certificate audit step, the audit apparatus applies a digital signature on the audit result.

23. An event-ordering certification apparatus connected to both a user apparatus performing an event-ordering request for certifying a chronological sequence of a certain event in time-series events generating a designated digital

information thereby promoting the event-ordering certification apparatus to draft a certificate and an audit apparatus for auditing authenticity of the certificate through a communication network mutually, for drafting the certificate, for the event-ordering request of the user apparatus, the event-ordering certification apparatus comprising:

event-ordering request receiving means configured to receive the event-ordering request from the user apparatus;

sequentially assigned data-item calculating means configured to draft a sequentially assigned data-item from a digital information included in the event-ordering request in accordance with a predetermined procedure;

event-ordering request aggregating means configured, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, to calculate assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

certificate drafting means configured to draft a certificate containing the sequentially assigned data-item and a first sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto;

certificate sending means configured to send the certificate to the user apparatus;

assuming that: a leaf of the sequential aggregation tree to which the event-ordering request is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the

certificate; and in the complementary information, a complementary information acquirable at a point of assigning the event-ordering request to the sequential aggregation tree is defined as an immediate complementary information,

audit certificate drafting means configured, after assigning the event-ordering request to the sequential aggregation tree, to assign a first audit request to the sequential aggregation tree thereby drafting a first audit certificate in the same way as drafting the certificate, acquire a first immediate complementary information for audit at the point of assigning the first audit request to the sequential aggregation tree, from the sequential aggregation tree and incorporate the first immediate complementary information into the first audit certificate;

audit certificate sending means configured to send the first audit certificate to the audit apparatus;

complementary information request receiving means configured, after assigning the first audit request to the sequential aggregation tree, to receive a request of the complementary information of the certificate from the user apparatus;

late complementary information drafting means configured to acquire a second sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the request of the complementary information assigned thereto and a complementary information acquirable at the point of assigning the request of the complementary information, from the sequential aggregation tree, thereby forming a late complementary information; and

complementary information sending means configured to send the late complementary information about the certificate to the user apparatus.

24. The event-ordering certification apparatus of claim 23, wherein the certificate drafting means incorporates the immediate complementary information of the certificate into the first sequential aggregation tree specifying information.

25. The event-ordering certification apparatus of claim 23 or 24, wherein:

the audit certificate drafting means further includes means configured, before assigning the event-ordering request to the sequential aggregation tree, to assign a second audit request to the sequential aggregation tree thereby drafting a second audit certificate in the same way as drafting the certificate, acquire a second immediate complementary information for audit at the point of assigning the second audit request to the sequential aggregation tree from the sequential aggregation tree and incorporate the second immediate complementary information into the second audit certificate; the event-ordering certification apparatus further comprises:

an audit late complementary information drafting means configured, after completing the regular time interval, to acquire all of the complementary information about the first and second audit certificates drafted at the audit certificate drafting step, from the sequential aggregation tree thereby forming a late complementary information about the first and second audit certificates; and

an audit late complementary information sending means configured to send the late complementary information about the first and second audit certificates to the audit apparatus.

26. The event-ordering certification apparatus of any one of claims 23 to 25, wherein the sequentially assigned data-item calculating means calculates a result value obtained by applying a designated collision-resistant hash function on the digital information contained in the event-ordering request, as the sequentially assigned data-item.

27. The event-ordering certification apparatus of any one of claims 23 to 26, wherein the certificate drafting means applies a digital signature on the certificate drafted.

28. The event-ordering certification apparatus of any one of claims 23 to 27,

further comprising electronic information publishing means configured to publish the root value of the sequential aggregation tree electronically after completing the regular time interval.

29. The event-ordering certification apparatus of any one of claims 23 to 28, wherein for a plurality of event-ordering requests from the user apparatus, the certificate sending means further includes means configured to send respective certificates for the event-ordering requests in chronological sequence of assigning the event-ordering requests to the sequential aggregation tree.

30. The event-ordering certification apparatus of claim 24, further comprising, for a plurality of event-ordering requests from the user apparatus:

sequential aggregation tree storing means configured to store an information about the sequential aggregation tree produced at the event-ordering request aggregating step; and,

assuming that: the late complementary information of a leaf a1 determined at the point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

registration point storing means configured to store an information about the registration points of the plural event-ordering requests, wherein

the certificate drafting means integrates, from the information stored by both of the sequential aggregation tree storing means and the registration point storing means, the sequential assigned data-item of the new registration point, the first sequential aggregation tree specifying information for specifying the sequential aggregation tree and the leaf thereof both having the sequentially assigned data-item assigned thereto, the immediate complementary information of the new registration point and the late complementary information of all of the

passed registration points of the user apparatus at the new registration point, thereby drafting a certificate for the new registration point.

31. The event-ordering certification apparatus of claim 24, further comprising, for a plurality of event-ordering requests from the user apparatus,

sequential aggregation tree storing step means configured to store an information about the sequential aggregation tree produced at the event-ordering request aggregating means; and,

assuming that: the late complementary information of a leaf a1 determined at the point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

registration point storing means configured to store an information about an immediately preceding registration point to the new registration point, wherein

the certificate drafting means integrates, from the information stored by both of the sequential aggregation tree storing means and the registration point storing means, the sequential assigned data-item of the new registration point, the sequential aggregation tree specifying information for specifying the sequential aggregation tree and the leaf thereof both having the sequentially assigned data-item assigned thereto, the immediate complementary information of the new registration point and the late complementary information of the immediately preceding registration point of the user apparatus at the new registration point, thereby drafting a certificate for the new registration point.

32. The event-ordering certification apparatus of claim 30 or 31, wherein the sequential aggregation tree storing means stores respective positions of nodes in the sequential aggregation tree, which have been subjected to an assignation, and respective assigned values for the nodes, as the information about the sequential

aggregation tree.

33. The event-ordering certification apparatus of claim 31, wherein the sequential aggregation tree storing means includes a first stack to store the immediate complementary information of the new registration point and a second stack to store the late complementary information of the immediately preceding registration point of the user apparatus at the new registration point.

34. The event-ordering certification apparatus of any one of claims 30 to 33, further comprising electronic information publishing means configured to electronically publish the root value of the sequential aggregation tree after completing the regular time interval.

35. The event-ordering certification apparatus of any one of claims 30 to 34, wherein when the event-ordering certification apparatus stops an operation thereof or vanishes data necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval, the user apparatus further includes user's side electronic information publishing means configured to electronically publish both positional information and assigned values for one or more nodes whose assigned values are calculable and whose parents' assigned values are not calculable, from the certificates that the user apparatus has already received and stored by the time of stopping the operation of the certification apparatus or vanishing the data.

36. The event-ordering certification apparatus of any one of claims 30 to 35, wherein after completing the regular time interval, the event-ordering request aggregating means assigns the root value of the sequential aggregation tree to a leaf of a next sequential aggregation tree so as to form the immediate complementary information about a new registration point assigned to the leaf of the next sequential aggregation tree.

37. An event-ordering certification audit apparatus connected to both at least one user apparatus performing an event-ordering request for certifying a chronological sequence of a certain event in time-series events generating a designated digital information and a certification apparatus for drafting a certificate for the event-ordering request of the user apparatus, through a communication network, for auditing authenticity of the certificate, wherein the certification apparatus comprises:

event-ordering request receiving means configured to receive a first event-ordering request from the user apparatus;

sequentially assigned data-item calculating means configured to draft a sequentially assigned data-item from a digital information included in the first event-ordering request in accordance with a predetermined procedure;

event-ordering request aggregating means configured, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, to calculate assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

certificate drafting means configured to draft a first certificate containing the sequentially assigned data-item and a first sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto;

certificate sending means configured to send the first certificate to the user apparatus;

assuming that: a leaf of the sequential aggregation tree to which the first

event-ordering request is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the first certificate; and in the complementary information, a complementary information acquirable at a point of assigning the first event-ordering request to the sequential aggregation tree is defined as an immediate complementary information,

audit certificate drafting means configured to assign a plurality of audit requests to the sequential aggregation tree thereby drafting a plurality of audit certificates in the same way as drafting the certificate, acquire immediate complementary information for audit at the point of assigning the respective audit requests to the sequential aggregation tree from the sequential aggregation tree and incorporate the immediate complementary information for audit into the respective audit certificates;

audit certificate sending means configured to send the audit certificates to the audit apparatus;

complementary information request receiving means configured, after sending the first certificate to the user apparatus, to receive a request of the complementary information of the first certificate from the user apparatus;

late complementary information drafting means configured to acquire a second sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the request of the complementary information assigned thereto and a complementary information acquirable at the point of assigning the request of the complementary information, from the sequential aggregation tree, thereby forming a late complementary information; and

late complementary information sending means configured to send the late complementary information about the first certificate to the user apparatus, and

wherein the event-ordering certification audit apparatus comprises:

audit certificate receiving means configured to receive the audit

certificates from the certification apparatus;

audit request receiving means configured to receive an audit request for the first certificate from the user apparatus, the audit request containing the first certificate and the late complementary information about the first certificate;

first audit certificate selecting means configured to select an audit certificate from the audit certificates on a basis of the first and second sequential aggregation tree specifying information in the audit request for the first certificate, the audit certificate being generated after the first certificate and before the late complementary information in chronological sequence;

first certificate audit means configured to audit validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit certificate selected by the first audit certificate selecting means coincides with an assigned value for the specified node calculated from the audit request for the first certificate or not and, also configured to further certify a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt time of the audit request for the audit certificate selected by the first audit certificate selecting means; and

audit result sending means configured to send an audit result of the first certificate to the user apparatus.

38. The event-ordering certification audit apparatus of claim 37, wherein:

the audit certificate receiving means further includes means configured to acquire a first time when the audit apparatus received the audit certificate selected by the first audit certificate selecting means, from a time offering apparatus; and

the first certificate audit means incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first certificate is temporally ahead of the first time into the audit result.

39. The event-ordering certification audit apparatus of claim 37 or 38, wherein

the certification apparatus further comprises:

audit late complementary information drafting means configured to acquire all of the complementary information about the audit certificates drafted by the audit certificate drafting means from the sequential aggregation tree after completing the regular time interval, thereby forming a late complementary information about the audit certificates; and

audit late complementary information sending means configured to send the late complementary information about the audit certificates to the audit apparatus, and

wherein the event-ordering certification audit apparatus further comprises:

second audit certificate selecting means configured to select an audit certificate from the audit certificates on a basis of the first sequential aggregation tree specifying information in the audit request for the first certificate, the audit certificate being generated before the first certificate in chronological sequence; and

second certificate audit means configured to audit validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit request for the first certificate coincides with an assigned value for the specified node calculated from the audit certificate selected by the second audit certificate selecting means and the late complementary information in the audit certificate or not and, where the audit apparatus further certifies a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt time of the audit request for the audit certificate selected by the second audit certificate selecting means.

40. The event-ordering certification audit apparatus of claim 39, further comprising, for a second event-ordering request from the user apparatus or the other user apparatus, inter-certificate ordering judgment means configured to judge the temporal context between the receipt time of the event-ordering request for the

first certificate and the receipt time of the event-ordering request for the second certificate on a basis of validation of the audit result for the second certificate drafted for the second event-ordering request and the first sequential aggregation tree specifying information about the first and second certificates, wherein

the audit result sending means incorporates a chronological sequence in receiving the requests in between the plural certificates into the audit result.

41. The event-ordering certification audit apparatus of claim 39 or 40, further comprising:

root-value calculating means configured to calculate a root value of the sequential aggregation tree from the plural audit certificates and the late complementary information about the plural audit certificates; and

root-value validation means configured to verify whether a root value of the sequential aggregation tree published electronically coincides with the root value calculated at the root-value calculating step.

42. The event-ordering certification audit apparatus of any one of claims 39 to 41, further comprising audit complementary information sending means configured to send the audit certificate selected by the first audit certificate selecting means and the late complementary information about the audit certificate to the user apparatus.

43. The event-ordering certification audit apparatus of any one of claims 39 to 42, wherein:

the audit certificate receiving means further includes means configured to acquire a second time when the event-ordering certification audit apparatus sent the audit certificate selected by the second audit certificate selecting means to the user apparatus, from a time offering apparatus; and

the second certificate audit means incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first

certificate is temporally ahead of the second time into the audit result.

44. The event-ordering certification audit apparatus of any one of claims 39 to 42, wherein the first certificate audit means applies a digital signature on the audit result.

45. An event-ordering certification program for allowing the certification apparatus to perform the respective steps of the event-ordering certification method of any one of claims 1 to 14.

46. An event-ordering certification audit program for allowing the certification apparatus to perform the respective steps of the event-ordering certification audit method of any one of claims 15 to 22.

47. A program for validation of event-ordering certificates for a user apparatus in an event-ordering certification audit system where at least one user apparatus performing an event-ordering request for certifying a chronological sequence of a certain event in time-series events generating a designated digital information, a certification apparatus for drafting a certificate for the event-ordering request of the user apparatus and an audit apparatus for auditing authenticity of the certificate are connected with each other through a communication network,

wherein the certification apparatus comprises:

event-ordering request receiving means configured to receive a first event-ordering request from the user apparatus;

sequentially assigned data-item calculating means configured to draft a sequentially assigned data-item from a digital information included in the first event-ordering request in accordance with a predetermined procedure;

event-ordering request aggregating means configured, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a

directed tree from left thereof, to calculate assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

certificate drafting means configured to draft a first certificate containing the sequentially assigned data-item and a first sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto;

certificate sending means configured to send the first certificate to the user apparatus;

assuming that: a leaf of the sequential aggregation tree to which the first event-ordering request is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the first certificate; and in the complementary information, a complementary information acquirable at a point of assigning the first event-ordering request to the sequential aggregation tree is defined as an immediate complementary information,

audit certificate drafting means configured to assign a plurality of audit requests to the sequential aggregation tree thereby drafting a plurality of audit certificates in the same way as drafting the certificate, acquire immediate complementary information for audit at the point of assigning the respective audit requests to the sequential aggregation tree from the sequential aggregation tree and incorporate the immediate complementary information for audit into the respective audit certificates;

audit certificate sending means configured to send the audit certificates to the audit apparatus;

complementary information request receiving means configured, after

sending the first certificate to the user apparatus, to receive a request of the complementary information of the first certificate from the user apparatus;

late complementary information drafting means configured to acquire a second sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the request of the complementary information assigned thereto and a complementary information acquirable at the point of assigning the request of the complementary information, from the sequential aggregation tree, thereby forming a late complementary information; and

late complementary information sending means configured to send the late complementary information about the first certificate to the user apparatus, and

wherein the audit apparatus comprises:

audit certificate receiving means configured to receive the audit certificates from the certification apparatus;

audit request receiving means configured to receive an audit request for the first certificate from the user apparatus, the audit request containing the first certificate and the late complementary information about the first certificate;

first audit certificate selecting means configured to select an audit certificate from the audit certificates on a basis of the first and second sequential aggregation tree specifying information in the audit request for the first certificate, the audit certificate being generated after the first certificate and before the late complementary information in chronological sequence;

first certificate audit means configured to audit validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit certificate selected by the first audit certificate selecting means coincides with an assigned value for the specified node calculated from the audit request for the first certificate or not and, also configured to further certify a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt

time of the audit request for the audit certificate selected by the first audit certificate selecting means; and

audit result sending means configured to send an audit result of the first certificate to the user apparatus, and

wherein the event-ordering certification program allows the user apparatus to perform:

an event-ordering request sending step of sending the first event-ordering request to the certification apparatus;

a certificate receiving step of receiving first event-ordering request from the certification apparatus

a complementary information request sending step of sending the request of the complementary information of the first certificate to the certification apparatus;

a complementary information receiving step of receiving the complementary information of the first certificate from the certification apparatus;

an audit request sending step of sending the audit request to the audit apparatus; and

an audit result receiving step of receiving the audit result for the first certificate.

48. The program for validation of event-ordering certificates of claim 47, wherein:

the audit certificate receiving means further includes means configured to acquire a first time when the audit apparatus received the audit certificate selected by the second audit certificate selecting means from a time offering apparatus; and

the first certificate audit means incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first certificate is temporally ahead of the first time into the audit result, and

wherein the program for validation of event-ordering certificates allows the user apparatus to perform an event-ordering request drafting step of acquiring a

third time at the point of sending the first event-ordering request to the certification apparatus from the time offering apparatus and incorporating a value as a result of calculating the third time in accordance with a designated procedure into the first event-ordering request.

49. The program for validation of event-ordering certificates of claim 47 or 48, wherein the certification apparatus further comprises:

audit late complementary information drafting means configured to acquire all of the complementary information about the audit certificates drafted by the audit certificate drafting means from the sequential aggregation tree after completing the regular time interval, thereby forming a late complementary information about the audit certificates; and

audit late complementary information sending means configured to send the late complementary information about the audit certificates to the audit apparatus, and

wherein the audit apparatus further comprises:

second audit certificate selecting means configured to select an audit certificate from the audit certificates on a basis of the first sequential aggregation tree specifying information in the audit request for the first certificate, the audit certificate being generated before the first certificate in chronological sequence; and

second certificate audit means configured to audit validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit request for the first certificate coincides with an assigned value for the specified node calculated from the audit certificate selected by the second audit certificate selecting means and the late complementary information in the audit certificate or not and, where the audit apparatus further certifies a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt time of the audit request for the audit certificate selected by the second audit certificate

selecting means.

50. The program for validation of event-ordering certificates of claim 49, wherein:

the audit apparatus includes, for a second event-ordering request from the user apparatus or the other user apparatus, inter-certificate ordering judgment means configured to judge the temporal context between the receipt time of the event-ordering request for the first certificate and the receipt time of the event-ordering request for the second certificate on a basis of validation of the audit result for the second certificate drafted for the second event-ordering request and the first sequential aggregation tree specifying information about the first and second certificates;

the audit result sending means incorporates a chronological sequence in receiving the requests in between the first and second certificates into the audit result; and

the audit request for the first certificate includes a request for judging its chronological sequence in relation to the second certificate.

51. The program for validation of event-ordering certificates of claim 49, wherein:

the audit apparatus includes audit complementary information sending means configured to send the audit certificate selected by the first audit certificate selecting means and the late complementary information about the audit certificate to the user apparatus; and

the program for validation of event-ordering certificates allows the user apparatus to perform a step of receiving the audit certificate and its late complementary information sent from the audit apparatus.

52. The program for validation of event-ordering certificates of any one of claims 48 to 51, wherein:

the audit certificate receiving means further includes means configured to acquire a second time when the event-ordering certification audit apparatus sent the audit certificate selected by the second audit certificate selecting means to the user apparatus, from a time offering apparatus;

the second certificate audit means incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first certificate is temporally ahead of the second time into the audit result; and

the program for validation of event-ordering certificates allows the user apparatus to perform an event-ordering request drafting step of acquiring a third time at the point of sending the first event-ordering request to the certification apparatus from the time offering apparatus and incorporating a value as a result of calculating the third time in accordance with a designated procedure into the first event-ordering request.

53. The program for validation of event-ordering certificates of any one of claims 47 to 52, wherein the program for validation of event-ordering certificates allows the user apparatus to perform:

a root-value calculating step of calculating a root value of the sequential aggregation tree from the first certificate sent from the certification apparatus and all of the late complementary information about the first certificate acquired after completing the regular time interval; and

a root-value validation step of verifying whether a root value for the sequential aggregation tree published electronically after completing the regular time interval coincides with the root value calculated at the root-value calculating step.

54. A program for validation of event-ordering certificates for allowing a computer to verify authenticity of certificates, the computer being connected to first and second user apparatuses, each of which performs an event-ordering request for certifying a chronological sequence of a certain event in time-series

events generating a designated digital information, and an event-ordering certification apparatus for drafting the certificates for a plurality of event-ordering requests of the first and second user apparatuses through a communication network,

wherein the event-ordering certification apparatus comprises:

event-ordering request receiving means configured to receive the event-ordering requests from the first and second user apparatuses;

sequentially assigned data-item calculating means configured to draft sequentially assigned data-items from digital information included in the event-ordering requests in accordance with a predetermined procedure;

event-ordering request aggregating means configured, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, to calculate assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

sequential aggregation tree storing means configured to store an information about the sequential aggregation trees produced by the event-ordering request aggregating means;

assuming that: a leaf of the sequential aggregation tree to which the sequentially-assigned data-item drafted from each of the event-ordering requests is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the registration point; in the complementary information, a complementary information acquirable at a point of assigning each of the sequentially assigned data-item to the sequential aggregation

tree is defined as an immediate complementary information, while a complementary information acquirable after the point of assigning each of the sequentially assigned data-item to the sequential aggregation tree is defined as a late complementary information; the late complementary information of a leaf a1 determined at a point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

registration point storing means configured to store an information about the registration points of the event-ordering requests with respect to each of the user apparatuses;

certificate drafting means configured to integrate, from the information stored in the respective storing means, a sequentially assigned data-item for the new registration point, a sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto, an immediate complementary information about the new registration point and a late complementary information of all past registration points of each of the user apparatuses, thereby drafting a certificate for the new registration point; and

certificate sending means configured to send the certificates to the user apparatuses;

wherein each of the user apparatuses comprises:

event-ordering request sending means configured to send the event-ordering requests to the event-ordering certification apparatus;

certificate receiving means configured to receive the certificates for the event-ordering requests from the event-ordering certification apparatus;

certificate storing means configured to store the certificates received;

validation request sending means configured to send a certificate for validation to the computer; and

validation result receiving means configured to receive a validation result of the certificate for validation from the computer;

wherein the program for validation of event-ordering certificates allows the computer to perform:

a certificate receiving step of receiving two certificates for validation from the first and second user apparatuses respectively or two certificates for validation from the first user apparatus;

assuming that one of the two certificates judged as being temporally former in publishing order is a first certificate, while the other of the two certificates judged as being temporally latter in publishing order is a second certificate, based on the sequential aggregation tree specifying information of the two certificates received,

a sequential aggregation tree specifying information sending step of sending the sequential aggregation tree specifying information in the second certificate to the user apparatus receiving the first certificate;

a late complementary information receiving step of receiving the late complementary information about the first certificate at a registration point after publishing the second certificate, from the user apparatus receiving the first certificate;

a validation step of verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the second certificate coincides with an assigned value for the specified node calculated from the first certificate and the late complementary information or not, thereby certifying validity of the first and second certificates and that the registration point of the first certificate is temporally ahead of the registration point of the second certificate, based on a validation result; and

a validation result sending step of sending the validation result to both or either of the first and second user apparatuses.

55. The program for validation of event-ordering certificates of claim 54,

wherein when the event-ordering certification apparatus stops an operation thereof or vanishes data necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval,

each of the user apparatuses includes user's side electronic information publishing means configured to electronically publish both positional information and assigned values for one or more nodes whose assigned values are calculable and whose parents' assigned values are not calculable, from the certificates that the user apparatus has already received and stored by the time of stopping the operation of the certification apparatus or vanishing the data, and

when the event-ordering certification apparatus stops an operation thereof or vanishes data necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval, the program for validation of event-ordering certificates allows the computer to perform a "by user's side publishing value" validation step of verifying that both received data at the certificate receiving step and received data at the late complementary information receiving step are not tampered by judging whether each assigned value for the one or more nodes published by the user apparatus through the user's side electronic information publishing means coincides with an assigned value calculated by both the received data at the certificate receiving step and the received data at the late complementary information receiving step.

56. A program for validation of event-ordering certificates for allowing a computer to verify authenticity of certificates, the computer being connected to first and second user apparatuses, each of which performs an event-ordering request for certifying a chronological sequence of a certain event in time-series events generating a designated digital information, and an event-ordering certification apparatus for drafting the certificates for a plurality of event-ordering requests of the first and second user apparatuses through a communication network,

wherein the event-ordering certification apparatus comprises:

event-ordering request receiving means configured to receive the event-ordering requests from the first and second user apparatuses;

sequentially assigned data-item calculating means configured to draft sequentially assigned data-items from digital information included in the event-ordering requests in accordance with a predetermined procedure;

event-ordering request aggregating means configured, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, to calculate assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

sequential aggregation tree storing means configured to store an information about the sequential aggregation trees produced by the event-ordering request aggregating means;

assuming that: a leaf of the sequential aggregation tree to which the sequentially-assigned data-item drafted from each of the event-ordering requests is assigned is defined as a registration point; an information about other nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the registration point; in the complementary information, a complementary information acquirable at a point of assigning each of the sequentially assigned data-item to the sequential aggregation tree is defined as an immediate complementary information, while a complementary information acquirable after the point of assigning each of the sequentially assigned data-item to the sequential aggregation tree is defined as a late complementary information; the late complementary information of a leaf a1 determined at a point of completing an assignation for a leaf a2 on the right of the

leaf a1 in the sequential aggregation tree is defined as "late complementary information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

registration point storing means configured to store an information about an immediately preceding registration point with respect to each of the user apparatuses;

certificate drafting means configured to integrate, from the information stored in the respective storing means, a sequentially assigned data-item for the new registration point, a sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto, an immediate complementary information about the new registration point and a late complementary information about the immediately preceding registration point of each of the user apparatuses at the new registration point, thereby drafting a certificate for the new registration point; and

certificate sending means configured to send the certificates to the user apparatuses;

defining that a rightmost registration point of the respective registration points of each of the user apparatuses is referred to as a provisional terminal point and that to calculate all of the complementary information about a designated registration point acquirable at a point of completing an assignment for the provisional terminal point is referred to as an incremental completion for a certificate of the designated registration point,

wherein each of the user apparatuses comprises:

event-ordering request sending means configured to send the event-ordering requests to the event-ordering certification apparatus;

certificate receiving means configured to receive the certificates for the event-ordering requests from the event-ordering certification apparatus;

certificate storing means configured to store the certificates received;

incremental completion means configured to perform the incremental completion to a certificate for validation of the plural certificates received and stored;

validation request sending means configured to send a certificate for validation to the computer; and

validation result receiving means configured to receive a validation result of the certificate for validation from the computer;

wherein the program for validation of event-ordering certificates allows the computer to perform:

a certificate receiving step of receiving two certificates for validation from the first and second user apparatuses respectively or two certificates for validation from the first user apparatus;

assuming that one of the two certificates judged as being temporally former in publishing order is a first certificate, while the other of the two certificates judged as being temporally latter in publishing order is a second certificate, based on the sequential aggregation tree specifying information of the two certificates received,

a sequential aggregation tree specifying information sending step of sending the sequential aggregation tree specifying information in the second certificate to the user apparatus receiving the first certificate;

a late complementary information receiving step of receiving the late complementary information about the first certificate at a registration point after publishing the second certificate, from the user apparatus receiving the first certificate;

a validation step of verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the second certificate coincides with an assigned value for the specified node calculated from the first certificate and the late complementary information or not, thereby certifying validity of the first and second certificates and that the registration point of the first certificate is temporally ahead of the registration point

of the second certificate, based on a validation result; and

a validation result sending step of sending the validation result to both or either of the first and second user apparatuses.

57. The program for validation of event-ordering certificates of claim 56, wherein when the event-ordering certification apparatus stops an operation thereof or vanishes data necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval,

each of the user apparatuses includes user's side electronic information publishing means configured to electronically publish both positional information and assigned values for one or more nodes whose assigned values are calculable and whose parents' assigned values are not calculable, from the certificates that the user apparatus has already received and stored by the time of stopping the operation of the certification apparatus or vanishing the data, and

when the event-ordering certification apparatus stops an operation thereof or vanishes data necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval, the program for validation of event-ordering certificates allows the computer to perform a "by user's side publishing value" validation step of verifying that both received data at the certificate receiving step and received data at the late complementary information receiving step are not tampered by judging whether each assigned value for the one or more nodes published by the user apparatus through the user's side electronic information publishing means coincides with an assigned value calculated by both the received data at the certificate receiving step and the received data at the late complementary information receiving step.

58. The program for validation of event-ordering certificates of claim 47, wherein the certification apparatus further comprising, for a plurality of event-ordering requests from the user apparatus:

sequential aggregation tree storing means configured to store an

information about the sequential aggregation tree produced by the event-ordering request aggregating means;

assuming that: the late complementary information of a leaf a1 determined at the point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

registration point storing means configured to store an information about the immediately preceding registration point,

certificate drafting means configured to integrate, from the information stored in the respective storing means, a sequentially assigned data-item for the new registration point, a sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto, an immediate complementary information about the new registration point and a late complementary information about the immediately preceding registration point of each of the user apparatuses at the new registration point, thereby drafting a certificate for the new registration point; and

certificate sending means configured to send the certificates to the user apparatuses; and

defining that a rightmost registration point of the respective registration points of each of the user apparatuses is referred to as a provisional terminal point and that to calculate all of the complementary information about a designated registration point acquirable at a point of completing an assignment for the provisional terminal point is referred to as an incremental completion for a certificate of the designated registration point, wherein the program for validation of event-ordering certificates allows the computer to perform:

an event-ordering request sending step of sending the event-ordering requests to the certification apparatus;

a certificate receiving step of receiving the certificates for the event-ordering requests from the certification apparatus;

a certificate storing step of storing the certificates received; and

an incremental completion step of performing the incremental completion to a certificate for validation of the plural certificates received and stored.

59. The program for validation of event-ordering certificates of any one of claims 56 to 58, wherein the incremental completion is carried out with the use of the certificates that the user apparatus received from the certification apparatus and further stored therein and without forming a tree structure.

60. The program for validation of event-ordering certificates of claim 59, wherein for respective elements forming the complementary information about a designated registration point acquirable at a point of completing an assignment for the provisional terminal point, the incremental completion is carried out by firstly selecting one certificate out of one or more certificates that the user apparatus received from the certification apparatus and further stored therein, the one certificate containing either the elements directly or information enough to calculate the elements, and secondly calculating the elements from the one certificate selected.

61. The program for validation of event-ordering certificates of claim 59, wherein the complementary information is carried out to all of registration points positioned on the left of the provisional terminal point of the user apparatus.

62. The program for validation of event-ordering certificates of claim 61, defining that, for one registration point a1 of the user apparatus on the left of the provisional terminal point and another registration point a2 of the user apparatus closest to the point a1 on a left side thereof, to calculate all of the complementary information about the registration point a2 acquirable at a point of completing an

assignment of the provisional point from all of the complementary information about the registration point a1 acquirable at the point of completing the assignment of the provisional point and receipts at the registration points a1 and a2, is referred to as a propagation procedure for completion, wherein

the incremental completion is carried out without forming a tree structure by the steps of:

originating in calculating or acquiring all of the complementary information about a registration point a of the user apparatus, which information is acquirable at a point of completing the assignment of the provisional terminal point, from the certificate that the user apparatus received and stored, the registration point a being closest to the provisional terminal point on a left side thereof;

starting a calculating process of all of the complementary information about respective registration points on the left of the provisional terminal point, which information is acquirable at a point of completing an assignment of the provisional terminal point, from a rightmost registration point a of the registration points; and

applying the calculating process on the registration points on the left of the registration point a in sequence while using the propagation procedure for completion.

63. The program for validation of event-ordering certificates of any one of claims 56 to 62, wherein the incremental completion is accomplished by a method comprising the steps of:

extracting respective registration points up to the provisional terminal point appropriately;

dividing into local areas each between the registration points extracted;

performing an incremental completion on the assumption that a rightmost assigned registration point in each of the local areas is a provisional terminal point; and

calculating all of acquirable complementary information about the extracted registration points.

64. The program for validation of event-ordering certificates of any one of claims 56 to 63, wherein

the certification apparatus has electronic information publishing means configured to publish the root value of the sequential aggregation tree electronically after completing the regular time interval; and

the program for validation of event-ordering certificates allows the user apparatus to perform:

a root-value calculating step of calculating a root value of the sequential aggregation tree from an information about the designated registration point and the complementary information calculated at the incremental completion step after completing the regular time interval; and

a root-value validation step of verifying whether the root value published electronically coincides with the root value calculated.

65. An event-time validation program readable by a computer that verifies a time when the user apparatus executing the program for validation of event-ordering certificates of claim 48 or 52 applies on the event-ordering request, wherein the event-time validation program allows the computer to perform:

an audit result acquiring step of acquiring the audit result;

an event-ordering request acquiring step of acquiring the event-ordering request corresponding to the audit result;

a time validation step of judging validity of the third time on a basis of a time difference between the third time and at least either the first time or the second time; and

a step of outputting the judgment.